

ANÁLISIS DE RIESGOS, AMENAZAS Y VULNERABILIDADES DE LA  
COMPAÑÍA PINZÓN PINZÓN & ASOCIADOS EN SU ÁREA DE TI Y  
PLANTEAMIENTO DE LOS CONTROLES A APLICAR BASADOS EN LA NORMA  
ISO 27001:2013.

ALEJANDRO JIMÉNEZ  
LEIDY XIMENA SALAZAR BARRERA

UNIVERSIDAD PILOTO DE COLOMBIA  
PROGRAMA DE INGENIERÍA DE SISTEMAS  
PROYECTO  
BOGOTÁ  
2016

ANÁLISIS DE RIESGOS, AMENAZAS Y VULNERABILIDADES DE LA  
COMPAÑÍA PINZÓN PINZÓN & ASOCIADOS EN SU ÁREA DE TI Y  
PLANTEAMIENTO DE LOS CONTROLES A APLICAR BASADOS EN LA NORMA  
ISO 27001:2013.

ALEJANDRO JIMÉNEZ  
LEIDY XIMENA SALAZAR BARRERA

TRABAJO DE GRADO

ASESOR  
JUAN CARLOS ALARCÓN SUESCÚN

UNIVERSIDAD PILOTO DE COLOMBIA  
PROGRAMA DE INGENIERÍA DE SISTEMAS  
PROYECTO  
BOGOTÁ  
2016

Nota de Aceptación:

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Bogotá, 21 de junio de 2016

## **DEDICATORIA**

*Este logro se lo dedico a mis padres JOSE OCTAVIO JIMENEZ GOMEZ y LUZ HELENA GARCIA MEJIA que me han impulsado y apoyado en todos los proyectos que he llevado a cabo en mi vida, a mi hija ISABELLA JIMENEZ MARIN que ha sido el gran motor de superación y de cambio para ser un mejor padre e individuo en la sociedad, a mi hermana LINA MARIA JIMENEZ GARCIA que me ha aconsejado y apoyado en las labores de emprendimiento realizadas.*

**Alejandro Jiménez**

*La culminación de esta etapa se la debo a mi familia la cual siempre me ha apoyado en todos mis proyectos y sueños, este es un gran logro que comparto con ellos y a los cuales les dedico esta meta cumplida.*

**Ximena Salazar**

## **AGRADECIMIENTOS**

Damos gracias a las personas que, de una u otra manera, han sido claves para lograr esta meta profesional, especialmente a nuestro director de trabajo de grado JUAN CARLOS ALARCON SUESCUN, el cual nos alentó a continuar y nos orientó de la mejor manera para salir adelante con este proyecto.

De igual manera damos gracias a nuestros familiares que son el motor de muchos de nuestros proyectos.

## CONTENIDO

	pág.
INTRODUCCIÓN	13
JUSTIFICACIÓN	15
1. PLANTEAMIENTO DEL PROBLEMA	16
1.1 DESCRIPCIÓN DEL PROBLEMA	16
1.2 FORMULACIÓN DEL PROBLEMA	16
1.3 TIPO DE ESTUDIO INVESTIGATIVO	16
1.3.1 Descriptivo.	16
1.4 FORMULACIÓN DE HIPÓTESIS	16
1.4.1 Hipótesis de investigación.	16
1.4.2 Hipótesis nula.	16
1.5 VARIABLES	16
1.5.1 Variable independiente.	17
1.5.2 Variables dependientes.	17
2. OBJETIVOS	18
2.1 GENERAL	18
2.2 ESPECÍFICOS	18
3. ALCANCES Y LIMITACIONES	19
3.1 ALCANCES	19
3.2 LIMITACIONES	20
4. MARCO REFERENCIAL	21
4.1 MARCO TEÓRICO	21
4.1.1 Seguridad de la información.	21

4.1.2 Análisis de riesgos informáticos.	23
4.1.3 Metodología de análisis de riesgos.	24
4.2 MARCO LEGAL	27
5. DESARROLLO DEL PROYECTO	28
5.1 CONTEXTO	28
5.1.1 Contexto legal.	29
5.1.2 Instalaciones.	30
5.1.3 Estructura de la red de Pinzón Pinzón & asociados.	30
5.1.4 Políticas de seguridad establecidas actualmente.	31
5.2 ANÁLISIS Y GESTIÓN DE RIESGOS	32
5.2.1 Norma.	32
5.2.2 Análisis de gestión de riesgo.	32
5.2.3 Identificación de activos.	33
5.2.4 Reporte de vulnerabilidades.	35
5.2.5 Valoración de activos.	37
5.2.6 Amenazas.	41
5.2.7 Valoración del impacto, probabilidad de ocurrencia.	42
5.2.8 Análisis GAP.	67
5.2.9 Determinación del riesgo.	77
5.2.10 Documento de declaración de aplicabilidad (SOA).	79
6. PLANES DE TRATAMIENTO	81
6.1 PLAN DE TRATAMIENTO N° 1	82
6.1.1 Seguridad física	83
6.2 PLAN DE TRATAMIENTO N° 2	83
6.2.1 Políticas de seguridad de usuarios	84

6.3 PLAN DE TRATAMIENTO N° 3	86
6.3.1 Políticas para realizar backups	86
6.4 PLAN DE TRATAMIENTO N° 4	88
6.4.1 Controles de cifrado de la información	89
6.4.2 Cifrado	89
6.4.3 Administración de claves	89
6.5 PLAN DE TRATAMIENTO N° 5	89
6.5.1 Políticas de contratación – recursos humanos	90
6.6 PLAN DE TRATAMIENTO N° 6	90
6.6.1 Política de monitoreo de base de datos	91
6.7 PLAN DE TRATAMIENTO N° 7	92
6.7.1 Seguridad en aplicaciones	93
6.7.2 Firewall, IDS e IPS	93
6.7.3 Proteger el código	94
6.7.4 Auditorías y análisis de vulnerabilidades periódicos	94
7. CONCLUSIONES Y RECOMENDACIONES	95
7.1 CONCLUSIONES	96
7.2 RECOMENDACIONES	98
BIBLIOGRAFÍA	100
CIBERGRAFÍA	101
ANEXOS	102



## LISTA DE FIGURAS

	pág.
Figura 1 Seguridad de la información según la norma ISO/IEC 17799	21
Figura 2 Esquema de gestión de riesgos	25
Figura 3 Fases PHVA	26
Figura 4 Estructura Organizacional	29
Figura 5 Instalaciones de la Compañía PINZÓN PINZÓN & ASOCIADOS	30
Figura 6 Estructura de la Red de PINZÓN PINZÓN & ASOCIADOS	31

## LISTA DE TABLAS

	pág.
Tabla 1 Valoración de los Activos	39
Tabla 2 Valoración del impacto y Probabilidad de Ocurrencia	43
Tabla 3 Gobierno y Responsabilidades de seguridad de la Información	68
Tabla 4 Recursos Humanos	69
Tabla 5 Gestión de Activos	69
Tabla 6 Control de Acceso	70
Tabla 7 Control de Cifrado	71
Tabla 8 Seguridad Física	71
Tabla 9 Seguridad en Operaciones	72
Tabla 10 Seguridad en las Comunicaciones	73
Tabla 11 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	73
Tabla 12 Relación con Proveedores	74
Tabla 13 Gestión de los incidentes de seguridad de la Información	75
Tabla 14 Aspectos de la Seguridad de la Información en la Gestión de Continuidad de Negocio	75
Tabla 15 Cumplimiento	76
Tabla 16 Promedio General de Cumplimiento Análisis GAP	76
Tabla 17 Determinación del riesgo	77
Tabla 18 Valoración del Riesgo	78

## LISTA DE CUADROS

	pág.
Cuadro 1 Roles Pinzón Pinzón & Asociados	28
Cuadro 2 Identificación de Activos	34
Cuadro 3 Reporte de Vulnerabilidades	35
Cuadro 4 Sugerencias para las vulnerabilidades encontradas	36
Cuadro 5 Escala Valorativa de Riesgos (Disponibilidad)	37
Cuadro 6 Valoración de Riesgos (Integridad)	37
Cuadro 7 Valoración de Riesgos (Confidencialidad)	38
Cuadro 8 Listado de Amenazas	41
Cuadro 9 Escala valorativa del impacto y Probabilidad de Ocurrencia	42
Cuadro 10 Escala Impacto	42
Cuadro 11 Valoración de la implementación por control	67
Cuadro 12 Análisis basados en SOA	79

## LISTA DE ANEXOS

	pág.
Anexo A GLOSARIO	1
Anexo B REPORTE DE VULNERABILIDADES	3
Anexo C DOCUMENTO DE DECLARACIÓN DE APLICABILIDAD (SOA)	9
Anexo D FORMATO POLÍTICA CONTRASEÑAS	19

## INTRODUCCIÓN

En la actualidad las empresas son más competitivas debido a que manejan grandes volúmenes de información,—almacenan información de sus clientes, actividades y datos personales, en general información confidencial, todo esto como operación del negocio, por lo cual se convierte en un riesgo la exposición de dicha información y la mala manipulación de la misma, por lo tanto es necesario establecer políticas, estándares necesarios que regulen de alguna manera la seguridad de esta.

Debido a los riesgos que se presentan en las organizaciones en la administración de la información y por ende la operación de la misma, es necesario implementar un análisis de riesgos basados en la normatividad ISO27001:2013 para diseñar las mejores estrategias que permitan contrarrestar las amenazas que puedan explotar las vulnerabilidades que puedan tener las organizaciones.

En la actualidad la empresa PINZÓN PINZÓN & ASOCIADOS en la ciudad de Bogotá, requiere de un análisis de riesgos para tener un panorama más amplio en cuanto a su estado en la seguridad de la información y así plantear un tratamiento adecuado para disminuir los riesgos a niveles aceptables para la compañía, estableciendo políticas y estándares necesarios que ayuden a minimizar el impacto que puede llegar a tener las fallas de seguridad en dicha compañía, para lo cual es indispensable el compromiso de la alta gerencia.

El siguiente estudio se llevará a cabo de acuerdo con a la normatividad ya antes descrita, adicionalmente se desarrollara un análisis de impacto, donde se clasificaran los procesos más críticos del área de TI. Se espera que la empresa pueda implementar los controles que se dejarán planteados al finalizar el proyecto y de esta manera puedan implementar un plan de continuidad el cual este bien soportado con estrategias que contribuyan a reducir, mitigar, aceptar o transferir los riesgos identificados.

Las normas internacionales ISO/IEC 27001 e ISO/IEC 27005 son los estándares elegidos para el desarrollo del trabajo, por su popularidad y gran aceptación a nivel mundial.

Es de vital importancia conocer el contexto de la organización para poder identificar cada elemento que pueda generar un riesgo en el departamento de TI, que en determinado momento pueda impactar la continuidad del negocio.

El primer paso que se realizará será conocer la empresa en su contexto, que se refiere a las actividades desarrolladas por la empresa como son: tipos de

clientes, tipo de información gestionada, tipo de actividad, estructura organizacional, número de funcionarios internos y externos, categorización de los funcionarios (cargos), centro de cómputo, aplicativos, planta física y políticas de seguridad existentes.

La identificación de cada riesgo permitirá identificar posibles vulnerabilidades de TI que puedan impactar el negocio y de acuerdo con los resultados se procederá a valorar el impacto y la probabilidad de que dichos eventos ocurran.

Al realizar la estimación de los riesgos se podrán evaluar los controles a implementar y si estos realmente son satisfactorios o no, esta es una revisión que se debe hacer constantemente. En el tratamiento de los riesgos se deben definir si estos son mitigables (implementando controles), trasladables (a un tercero), aceptables (si para la organización es muy costoso o la probabilidad de que ocurra es muy alta) o evitables (tomando políticas para que no suceda). Los riesgos son cambiantes por lo cual deben ser identificados y revaluados constantemente, ya que lo que hoy podría no ser un riesgo, mañana lo puede ser y con el incremento de nuevas tecnologías informáticas crece cada vez más el riesgo y cambian los modelos de gestión de información de las organizaciones.

El alcance de este trabajo no cubre la implementación, monitoreo o mantenimiento constante del proceso de gestión de riesgos, todas estas actividades serán responsabilidad de la empresa Pinzón Pinzón & Asociados Abogados una vez se presenten los resultados del análisis de riesgos de TI.

## **JUSTIFICACIÓN**

Debido a los diferentes incidentes que han afectado la organización en materia de seguridad, en diferentes periodos de tiempo y a que las medidas empleadas han sido insuficientes, se requiere realizar un análisis de riesgos y vulnerabilidades para identificar y tratar los riesgos a niveles aceptables.

La información almacenada en los servidores es de vital importancia para el día a día y se requiere brindar mayor seguridad en la operación de sus servicios.

Al identificar las vulnerabilidades (internas y externas) y realizar un análisis de riesgos, se podrán evidenciar deficiencias en el manejo de la seguridad de la información, que permitirán a la gerencia tomar medidas para mitigarlas, aceptando el riesgo residual del proceso.

Este proyecto permitirá mejorar y fortalecer la política de seguridad de información en toda la organización, para lo cual la organización debe implementar planes de sensibilización a los usuarios en el manejo de la información, que a futuro contribuirán a una mejor gestión de la información por parte de todo el personal de la organización

## **1. PLANTEAMIENTO DEL PROBLEMA**

### **1.1 DESCRIPCIÓN DEL PROBLEMA**

La empresa PINZON PINZON & ASOCIADOS, cuenta con diferentes sistemas de información los cuales han sido implementados sin un esquema especializado de seguridad. El tratamiento que se le ha dado a los problemas en seguridad de la información es insuficiente, generando brechas de seguridad, repetitivas en lapsos muy cortos sobre los que nunca se identifica su causa, ni se hace un seguimiento a las oportunidades de mejora.

### **1.2 FORMULACIÓN DEL PROBLEMA**

¿Qué plan se debe implementar para mitigar los riesgos en la organización PINZÓN PINZÓN & asociados en su área de TI y lograr su control a niveles aceptables?

### **1.3 TIPO DE ESTUDIO INVESTIGATIVO**

**1.3.1 Descriptivo.** Con este estudio se busca describir el análisis realizado a la compañía PINZÓN PINZÓN & ASOCIADOS, en el departamento de TI, y de allí poder obtener como resultado los riesgos, las vulnerabilidades y las amenazas que se presentan y de esta manera proponer un plan de controles los cuales ayudaran en la mitigación de los resultados obtenidos en el análisis.

### **1.4 FORMULACIÓN DE HIPÓTESIS**

**1.4.1 Hipótesis de investigación.** El análisis de riesgos, amenazas y vulnerabilidades para la organización PINZÓN PINZÓN & ASOCIADOS DE BOGOTÁ, logrará un diagnóstico que haga más factible la implementación de los controles a aplicar en su área de TI.

**1.4.2 Hipótesis nula.** El análisis de riesgos, amenazas y vulnerabilidades para la organización PINZÓN PINZÓN & ASOCIADOS DE BOGOTÁ, no logrará un diagnóstico que haga más factible la implementación de los controles a aplicar en su área de TI.

### **1.5 VARIABLES**

Dentro de la investigación se tendrán en cuenta dos tipos de variables dependientes e independientes, en donde el objetivo es que la variable independiente logre generar incidencia en la variable o las variables



dependientes, en este caso particular se logró determinar que existen 2 variables dependientes, las cuales tendrán determinado su comportamiento dependiendo de los alcances de la variable independiente; en este orden de ideas las variables están descritas de la siguiente manera:

**1.5.1 Variable independiente.** Análisis de riesgos para la organización PINZÓN PINZÓN & ASOCIADOS DE BOGOTÁ.

**1.5.2 Variables dependientes.**

- Resultados del diagnóstico de los riesgos, las amenazas y vulnerabilidades
- Planteamiento de los controles a aplicar.

## **2. OBJETIVOS**

### **2.1 GENERAL**

Realizar el análisis de riesgos, amenazas y vulnerabilidades para la compañía PINZÓN PINZÓN & ASOCIADOS, que permita el diagnóstico de las posibles amenazas y vulnerabilidades que presenta en su área de TI y plantear los controles a aplicar.

### **2.2 ESPECÍFICOS**

- Diagnosticar las posibles amenazas y vulnerabilidades que presentan en su área de TI la compañía PINZÓN PINZÓN & ASOCIADOS.
- Validar el análisis de gestión de riesgos por medio del informe que se presentará a la compañía y de esta manera validar el cumplimiento de las expectativas de la empresa PINZÓN PINZÓN & ASOCIADOS.
- Determinar los controles adecuados para su futura implementación.

### **3. ALCANCES Y LIMITACIONES**

#### **3.1 ALCANCES**

Los productos entregables están definidos de la siguiente manera:

Alcances del análisis de riesgos:

Contará con información detallada en los siguientes ítems:

- 1- Lista de activos relacionados con el proceso a evaluar.
- 2- Información de las amenazas que afectan cada activo involucrado en el proceso.
- 3- Información de las vulnerabilidades que contiene el proceso.
- 4- Probabilidad de ocurrencia.
- 5- Impacto para la organización.
- 6- Informe de los riesgos críticos que necesitan controles.
- 7- Planteamiento de los controles a aplicar de acuerdo al informe de riesgos, amenazas y vulnerabilidades.

Cabe resaltar que el análisis solo contendrá información relacionada con el proceso de TI.

Dentro del alcance para el proyecto se involucra uno de los objetivos el cual es a corto plazo, por otro lado se describe una de las limitaciones del alcance del proyecto.

El objetivo a corto plazo esta descrito de la siguiente manera:

- El diagnóstico de los riesgos, amenazas y vulnerabilidades permitirá generar un informe de la situación actual de la compañía y de esta manera poder plantear los pasos a seguir para que esta implemente los controles respectivos.

En segundo lugar se tiene la restricción que esta descrita de la siguiente manera:

- El alcance llega hasta el diseño de los controles por lo tanto se dejaran planteados los controles sugeridos para las amenazas que arroje el informe y la compañía ya se encargaría de la implementación a largo plazo.

### **3.2 LIMITACIONES**

Las limitaciones se encuentran relacionadas directamente con las actividades planteadas en el cronograma de trabajo previamente definido, y relaciona aspectos tales como:

- 1- El tiempo para desarrollar el análisis de riesgos.
- 2- El análisis de riesgos se enfocará únicamente al área de TI.
- 3- No se hará implementación de ningún control.

## 4. MARCO REFERENCIAL

### 4.1 MARCO TEÓRICO

**4.1.1 Seguridad de la información.** Se puede definir la seguridad de la información como el indicador del estado en el que se encuentran los datos en cuanto a seguridad, adicionalmente es la base por el cual se toman medidas de protección hacia estos y de esta manera se trata de evitar su pérdida, modificación o acceso no autorizado. Realizando este tipo de verificaciones aseguramos la no materialización de una amenaza que aprovecha las vulnerabilidades que pueden llegar a encontrar en los sistemas.

Las vulnerabilidades son todas aquellas debilidades que puedan llegar a afectar el funcionamiento directo o propiedad en sí de la información.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de la información.<sup>1</sup>

Estos pilares se pueden ver representados en la Figura 1 Seguridad de la información según la norma ISO/IEC 17799, en la cual se ve como estos salen de la información, la cual es el centro de ellos.

Figura 1 Seguridad de la información según la norma ISO/IEC 17799



Fuente: Enciclopedia de la seguridad informática. Pág. 5.

<sup>1</sup> MISFUD, Elvira. Introducción a la seguridad informática - Seguridad de la información / Seguridad informática, 26 de Marzo 2012. Monografía.[Online].; Disponible en: <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>

Garantizar un nivel de protección total es virtualmente imposible, la seguridad de la información en la práctica a un nivel total o de completitud no es alcanzable porque no existe un sistema seguro al ciento por ciento.<sup>2</sup>

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización<sup>3</sup> y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de los negocios. La información está expuesta a un mayor número de amenazas las cuales aprovechan las vulnerabilidades y de esta manera se exponen los activos, lo que puede poner en peligro la continuidad del negocio.

Según Hernando Ruíz.<sup>4</sup> "La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en cualquier tipo conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comunique o recolecte dicha información."

Las políticas de seguridad de una organización son las normas y procedimientos internos que deben seguir los integrantes de la organización para respetar los requerimientos de seguridad que deseen preservarse. Debe describirse la criticidad de los sistemas y de la información, los roles de cada puesto de trabajo y la mecánica de acceso a los sistemas, herramientas, documentación y cualquier otro componente del sistema de información<sup>5</sup>

La seguridad de la información es importante en empresas de todo tipo (público y privado), las cuales cada vez son más grandes y de acuerdo a su negocio le dan más importancia al resguardo de lo que representa para ellas las infraestructuras críticas.

"Realizar un plan de sensibilización y capacitación" <sup>6</sup> Esta estrategia es fundamental para la creación de un modelo de atención de incidentes, tiene como objetivo el de captar la atención de todos los miembros de la organización, es necesario comenzar al interior de la organización, se puede empezar desde las áreas gerenciales, administrativas, operativas, etc., e ir escalando y si fuera necesario incluir a los demás personas u organizaciones que tiene relación directa o indirecta, es decir en caso de los outsourcing, contratistas, temporales, etc.

---

<sup>2</sup> ISO 27000. Sistema de gestión de seguridad de la información. Términos de uso de la información. [en línea] <http://www.iso.org/iso/home/about.htm>

<sup>3</sup> ISO/IEC 13335-1:2004

<sup>4</sup> RUIZ L. Hernando. RESOLUCION 160-005326 Política de Seguridad de la información de la Superintendencia de Sociedades. 2008.

<sup>5</sup> Galdámez, Pablo, Seguridad Informática, Julio 2003, <http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf>

<sup>6</sup> Capítulo 1 Curso preparación CISM. Diplomado en Auditoría y Gestión de la Seguridad de la Información Gerencia de la seguridad de la información Auditoría interna de la norma ISO/IEC 27001:2013.

Es necesario que exista seguridad de la información en el área de TI de la organización PINZÓN PINZÓN & ASOCIADOS por las siguientes razones:

- Riesgos y Amenazas: Estafas, espionaje, daño, vandalismo, desastres naturales, hacking, virus, Denegación de servicio (DoS), etc.; Producto de diversas fuentes.
- Mayor vulnerabilidad a las amenazas por la dependencia de los sistemas y servicios de información conectados.
- Los sistemas de información no han sido diseñados con niveles de seguridad apropiados a los posibles riesgos informáticos existentes.

**4.1.2 Análisis de riesgos informáticos.** Para definir lo que es el análisis de riesgos, se debe puntualizar lo que es un riesgo, a continuación se exponen las siguientes definiciones:

Según Fernando Izquierdo Duarte<sup>7</sup> : “El riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos”.

Según Alberto Cancelado González<sup>8</sup>: "El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de las circunstancias del entorno, donde hay posibilidades de pérdidas"

Según Martín Vilches Troncoso<sup>9</sup>: "El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de objetivos y estrategias del negocio. Es decir es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no-ocurrencia de uno deseado”.

Teniendo en cuenta las definiciones anteriores el proceso de análisis de riesgos debe ser el más importante de la gestión de la seguridad de la información de una organización, de aquí parte la gestión de los riesgos, que es en últimas con la que se toman decisiones como: eliminarlos, ignorarlos, mitigarlos y controlarlos, es decir aplicar la gestión de riesgos basados en la

---

<sup>7</sup> IZQUIERDO D, Fernando. La administración y los riesgos. [online]. EN: Maxitana C, Jennifer D. (Auditor en control de gestión). Tesis: Administración de riesgos de tecnología de información de una empresa del sector informático. Guayaquil – Ecuador: Escuela Superior politécnica del Litoral, 2005. P.39. [http://www.cib.espol.edu.ec/Digipath/D\\_Tesis\\_PDF/D-33960.pdf](http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-33960.pdf)

<sup>8</sup> IZQUIERDO D, Fernando. La administración y los riesgos. [online]. EN: Maxitana C, Jennifer D. (Auditor en control de gestión). Tesis: Administración de riesgos de tecnología de información de una empresa del sector informático. Guayaquil – Ecuador: Escuela Superior politécnica del Litoral, 2005. P.39. [http://www.cib.espol.edu.ec/Digipath/D\\_Tesis\\_PDF/D-33960.pdf](http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-33960.pdf)  
<http://dspace.ucuenca.edu.ec/bitstream/123456789/2729/1/tm4487.pdf>

<sup>9</sup> VILCHES T, Martín. El riesgo [en line]. EN: Machuca C, John. (Magister en Contabilidad y Auditoría). Tesis Guía para la evaluación del sistema de riesgo operativo en la Cooperativa de Ahorro y Crédito Jardín Azuayo. Cuenca – Ecuador. Universidad de Cuenca, 2011. P.21. <http://dspace.ucuenca.edu.ec/bitstream/123456789/2729/1/tm4487.pdf>

compleja tarea de determinar, analizar, evaluar y clasificar los activos de información más importantes según la criticidad de los mismos, para este caso el área de TI de la compañía PINZÓN PINZÓN Y ASOCIADOS.

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, las vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.<sup>10</sup>

El resultado del análisis de riesgos se presenta en un documento comúnmente conocido como matriz de riesgos, pero pueden existir otras recomendaciones como informes de texto, diagramas de burbuja o mapas de calor. Como se describe en el estándar ISO / IEC 27001:2013.

Dentro del análisis de riesgos se encuentra la evaluación del riesgo que incluye las siguientes acciones y actividades.

- Identificación de los activos
- Identificación de los requisitos legales y de negocios que son relevantes para la identificación de los activos
- Valoración de los activos identificados: Teniendo en cuenta los requisitos legales identificados de negocios y el impacto de una pérdida de confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas y vulnerabilidades importantes para los activos identificados.
- Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cálculo del nivel del riesgo.
- Evaluación de los riesgos frente a una escala de riesgos preestablecidos.<sup>11</sup>

**4.1.3 Metodología de análisis de riesgos.** Las metodologías de análisis de riesgos de la información son desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de salvaguardas. Existen dos tipos: Las cuantitativas y las cualitativas, de las que existen gran cantidad de ambas clases a continuación se resume la metodología aplicada al caso de estudio específico en la compañía PINZÓN PINZÓN & ASOCIADOS.

La metodología que el proyecto adoptará será en base a la norma ISO 27005 e ISO 27001 (Norma de Análisis y Gestión de Riesgos de los Sistemas de Información y Norma de requisitos del SGSI): Dentro del esquema completo de etapas de ISO 27001 se encuentra el ciclo PHVA (Planear, Hacer, Verificar y Actuar), el cual puede aplicarse o no en su totalidad, para el caso de esta

---

<sup>10</sup> Wikipedia. Análisis de riesgo informático. [Online].; Disponible en: [http://es.wikipedia.org/wiki/Análisis\\_de\\_riesgo\\_informático](http://es.wikipedia.org/wiki/Análisis_de_riesgo_informático)

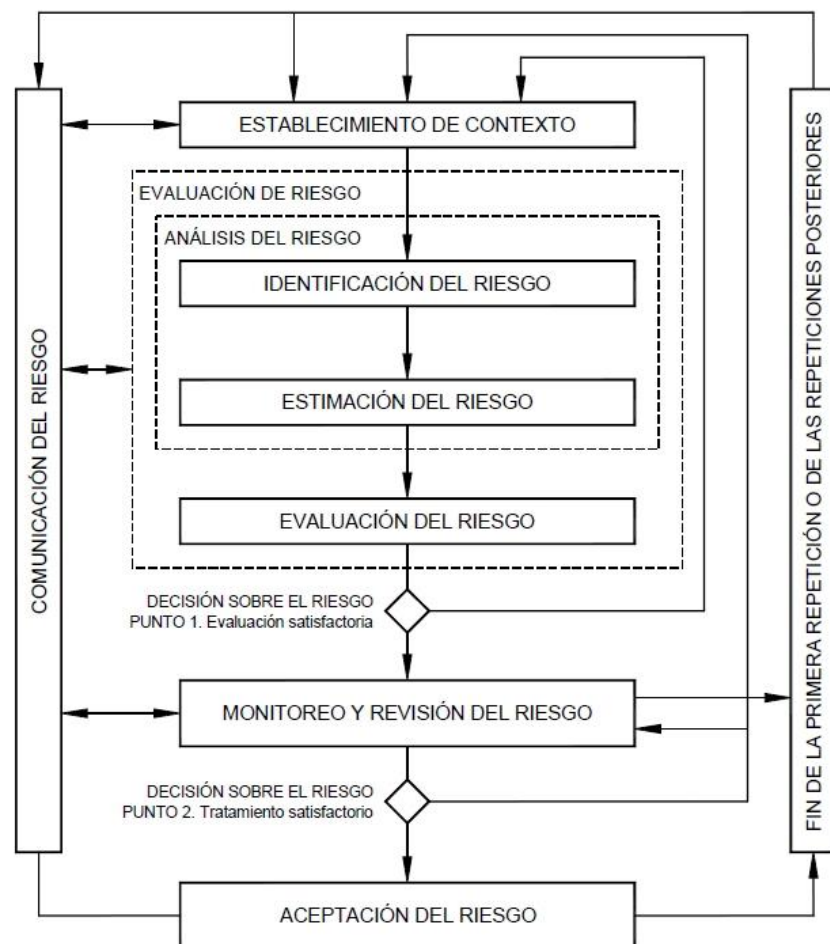
<sup>11</sup> BS ISO / IEC 27001:2013



compañía se llegará hasta el planteamiento de los controles a aplicar por lo tanto no se llegará a una implementación de los mismos.

Para tener claridad del esquema de gestión de riesgos se representó en la Figura 2 Esquema de gestión de riesgos, en la cual se presentan las diferentes etapas de este proceso donde el proyecto llegará hasta la evaluación del riesgo, ya que la implementación de controles se realizará por parte de la empresa a largo plazo, con su monitoreo y revisión constante del riesgo dependiendo si ha sido aceptado, mitigado, trasladado o evitado.

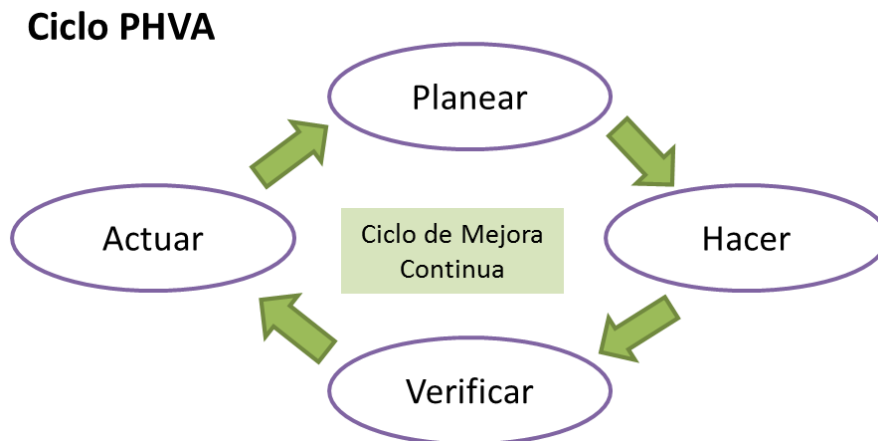
Figura 2 Esquema de gestión de riesgos



Fuente: INTERNATIONAL ORGANIZATION FOR STANDARIZATION.About ISO –ISO [En línea].  
<<http://www.iso.org/iso/home/about.htm>>

La siguiente Figura 3 Fases PHVA, muestra cómo sería el proceso utilizando dicha metodología en su totalidad:

Figura 3 Fases PHVA



FUENTE: Autores del proyecto (Basada en el modelo PDCA de Demming).

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001:2013, se utiliza el ciclo continuo PHVA, tradicional en los sistemas de gestión de la calidad.

**PLANIFICAR:** Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.<sup>12</sup>

Dentro de esta etapa se encuentran las siguientes actividades como fundamentales:

- Identificación de los riesgos: En esta etapa se identifican los activos, los propietarios de estos, las amenazas y vulnerabilidades de estos activos, el impacto en cuanto a la confidencialidad, integridad y disponibilidad de los activos.
- Analizar y evaluar los riesgos: Evaluar el impacto en el negocio de un fallo de seguridad, evaluar la probabilidad de ocurrencia, estimación de niveles de riesgo, determinar los criterios de aceptación del riesgo.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para aplicar controles adecuados, aceptación de riesgo de acuerdo a los criterios establecidos o en caso contrario evitarlos, mitigarlos o compartirlos.

**HACER:** Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información, para esto es necesario implantar un plan de tratamiento para los riesgos, implementar los controles previamente seleccionados, definir métricas para obtener resultados comparables,

<sup>12</sup> ISO 27001:2013, sección 6.1.1.

implementación de programas de concienciación, gestión de recursos para el mantenimiento de la seguridad de la información.

**VERIFICAR:** La organización deberá ejecutar procedimientos de monitorización y revisión para detectar a tiempo errores, brechas e incidentes de seguridad, determinar si las medidas correctivas tomadas fueron efectivas, todo esto mediante el uso de indicadores, los cuales permiten revisar regularmente el cumplimiento de las políticas y objetivos de SGSI, adicional medir la efectividad de los controles verificando así que se cumplen con los requisitos de seguridad, estas revisiones se deben realizar periódicamente, actualizando los cambios que se presenten y registrando las acciones y eventos que puedan haber afectado el rendimiento del SGSI.

**ACTUAR:** La organización deberá regularmente implantar en el SGSI las mejoras identificadas, realizar las acciones preventivas y correctivas, comunicar las acciones y mejoras a todas las partes interesadas, asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

Para el logro de objetivos del Plan de seguridad, se acordó con la organización realizar una reunión de inicio en la cual con apoyo del gerente asignado por parte de PINZÓN PINZÓN & ASOCIADOS, se conocieran detalles de los procesos involucrados por cada área, los perfiles y roles relacionados, las entradas y salidas de cada proceso y los productos o servicios misionales entregados por cada unidad.

## 4.2 MARCO LEGAL

Las Leyes, Decretos y demás documentación oficial que rigen el software emitida por el estado o los entes gubernamentales locales o regionales son:

- *LEY 1273 DE 2009*, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.<sup>13</sup>
- La Ley 1266 de 2008, también conocida como Ley de Habeas Data, se aplica a todos los datos personales financieros, crediticios, comerciales y de servicios registrados en un banco de datos. En este sentido, la aplicación de la Ley 1266 de 2008 está encaminada a regular el uso de esa información y por tanto otro tipo de datos (por ejemplo aquellos mantenidos en un ámbito exclusivamente personal o doméstico o los que se incluyen en una historia clínica) se encuentran excluidos de la aplicación de esta norma.

---

<sup>13</sup> Alcaldía de Bogotá. LEY 1273 DE 2009. [Online].; Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

## 5. DESARROLLO DEL PROYECTO

### 5.1 CONTEXTO

Pinzón Pinzón & Asociados es una firma de abogados, colombiana, fundada el 1º de mayo de 1988, conformada por un grupo de especialistas en las áreas de derecho corporativo, tributario, laboral, libre competencia, contratación pública, Propiedad Intelectual, Litigios y Asuntos Regulatorios.

La empresa Pinzón Pinzón & Asociados abogados tiene varias unidades de negocio (Asuntos regulatorios- Invima, Derecho Empresa, Litigios y Propiedad Intelectual), los cuales son prestados en nacionalmente e internacionalmente para cualquier cliente sin importar la actividad económica de este.

La información que maneja la firma es de carácter confidencial (actas, acuerdos, constitución de empresas, registro de productos, registros marcarios, etc.) por lo cual cualquier fuga de información puede comprometer la imagen de la misma con sus clientes, dentro de las leyes que rigen esta compañía y sus empleados están:

- La ley de HABEAS Data Ley 1581 de 2012
- Los decretos que las aclaran Decreto 1377 de 2013 y Decreto 886 de 2014.
- el artículo 74 de la Constitución Política habla del secreto profesional que aplica para la Firma de abogados y para los abogados que laboran allí.
- LEY 1123 DE 2007 Por la cual se establece el Código Disciplinario del Abogado.

Dentro de la compañía se tienen establecidos algunos roles los cuales se presentan a continuación:

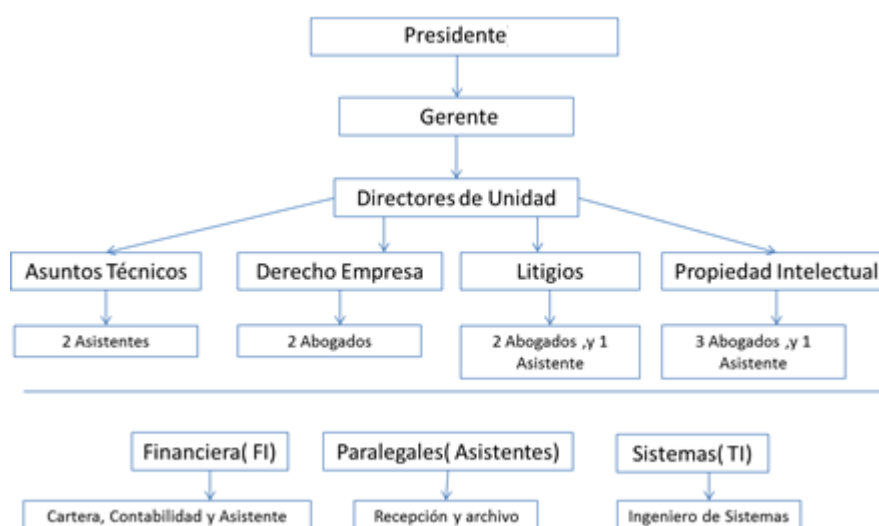
Cuadro 1 Roles Pinzón Pinzón & Asociados

Cantidad	Rol	Descripción Adicional
13	Abogados	1 Presidente, 1 Gerente, 4 Directores de Unidad y 7 abogados
4	Asistentes de las unidades	
2	Paralegales	Archivo y Recepción
3	Financiera	
1	Ingeniero de Sistemas	
Total: 23 funcionarios		

Fuente: Autores del Proyecto

La estructura organizacional de la firma se encuentra en la Figura 4 **¡Error! No se encuentra el origen de la referencia.**, en la cual se muestra la jerarquía y la cantidad de personas dentro de cada dependencia, esto se puede observar a continuación:

Figura 4 Estructura Organizacional



Fuente: Autores del Proyecto.

**5.1.1 Contexto legal.** Todas las empresa en Colombia deben regirse por la ley de HABEAS Data Ley 1581 de 2012 y los decretos que las aclaran Decreto 1377 de 2013 y Decreto 886 de 2014, adicionalmente el artículo 74 de la Constitución Política habla del secreto profesional que aplica para la Firma de abogados y para los abogados que laboran allí, como también LEY 1123 DE 2007 Por la cual se establece el Código Disciplinario del Abogado.

El secreto profesional (El secreto profesional en Colombia es inviolable por expresa disposición del artículo 74 de la Constitución Política) aplica para los abogados y está definido en el código disciplinario de los abogados que funciona durante y después de la cesación de sus servicios, con lo cual un juez de la republica podrá imponer o no una sanción disciplinaria y autorizar de manera excepcional al individuo a revelar la información para evitar la consumación de un delito.

La ley de protección de datos personales o habeas data, obliga a todas las empresas a generar medidas adecuadas de protección de la información personal que tengan a cargo, ya sea en archivos o en bases de datos.

Esta norma exige una serie de requisitos que las empresas deben cumplir con el objetivo de garantizar la protección de la información personal que tienen bajo su tratamiento. La ley aplica a las personas naturales y jurídicas que realicen tratamiento de datos personales.

Los datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquello que revelen el

origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

El no cumplimiento de ésta le podría acarrear fuertes sanciones, multas hasta de 2.000 SMLMV e incluso el cierre definitivo de las operaciones.

**5.1.2 Instalaciones.** Las oficinas de la empresa esta ubicadas en la ciudad de Bogotá, en la Calle 99 N 12 39 Piso 4, tel. 6219721, página web [www.pinzonpinzon.com](http://www.pinzonpinzon.com).

El centro de cómputo está ubicado en el lugar de las oficinas de la empresa, en un pequeño espacio cerca al área financiera a la vista y acceso del personal. En la Figura 5, se observa la distribución física de las instalaciones de la compañía, donde se resalta el área de TI, a la cual se le va a realizar el análisis a fondo.

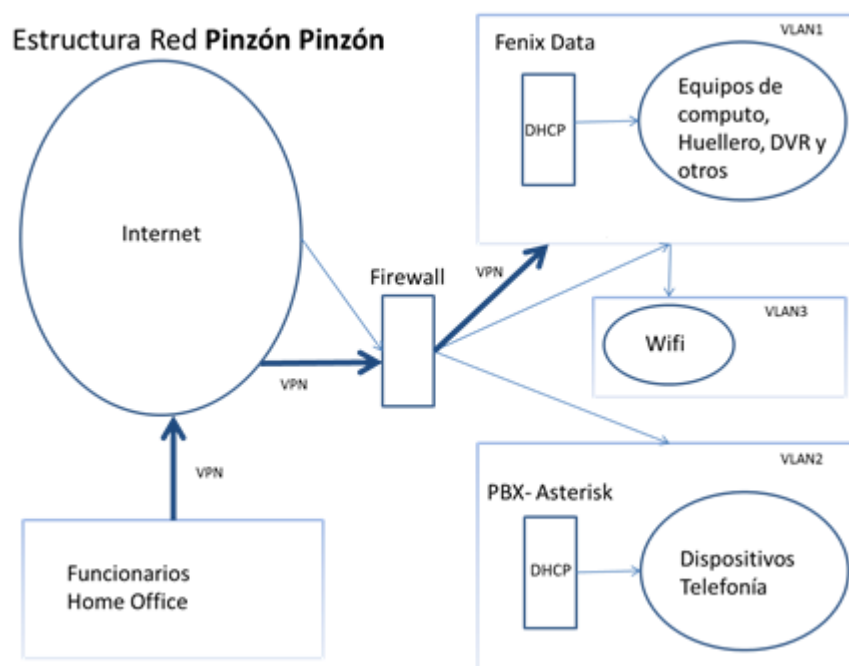
Figura 5 Instalaciones de la Compañía PINZÓN PINZÓN & ASOCIADOS



Fuente: Autores del proyecto

**5.1.3 Estructura de la red de Pinzón Pinzón & asociados.** Dentro del levantamiento de información que se realizó a la compañía uno de los puntos que se tuvo en cuenta fue la estructura de la red actual la cual se ve reflejada en la Figura 6 Estructura de la Red de PINZÓN PINZÓN & ASOCIADOS.

Figura 6 Estructura de la Red de PINZÓN PINZÓN & ASOCIADOS



Fuente: Autores del proyecto.

**5.1.4 Políticas de seguridad establecidas actualmente.** Las políticas existentes actualmente en la compañía se enumeran a continuación:

1. Acceso a través de Biométrico (Gestión).
2. Acceso a los servidores utilizando usuario y contraseña.
3. Backup Semanales Intercambio de discos.
4. Backup Internos incrementales.
5. Backup de configuración.
6. Creación de Cuentas (Correo y red) ingreso de personal y eliminación de cuentas.
7. Actualización de servidores y aplicaciones.

De acuerdo a la recolección de la información podemos comprobar que no existen políticas de seguridad oficiales, adicionalmente los controles básicos de acceso hacia el centro de datos de la compañía son muy bajos ya que la puerta que detiene la entrada puede ser vulnerada en cualquier momento puesto que no tiene ningún tipo de seguridad, adicional podemos ver que no se cuenta con un plan de contingencia ante desastres, no se ha realizado una evaluación de los riesgos que se tienen actualmente en la compañía y cuál puede ser el impacto que tendría en caso de materializarse algún ataque.

Estos son algunos de los motivos principales los cuales nos llevaron a realizar el proyecto continuando con la etapa de análisis y gestión de riesgos.

## 5.2 ANÁLISIS Y GESTIÓN DE RIESGOS

**5.2.1 Norma.** Debido al gran nivel de importancia que tiene la información de la compañía PINZÓN PINZÓN & ASOCIADOS, se optó por utilizar la norma ISO 27001:2013, ya que permitirá de alguna manera ponerles valor a los riesgos, adicional también permitirá saber cuánto de este valor está en juego, su impacto y según el nivel detectado ayudará a proteger la información.

Con la norma ISO 27001:2013 podemos:

- ✓ Concienciar a las altas directivas respecto al tema de la seguridad de la información.
- ✓ Concienciar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de prevenirlos a tiempo, teniendo unos controles que ayuden a mitigar estos riesgos.
- ✓ Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- ✓ Preparar a todos los interesados que interactúan en los procesos de TI, dentro de la organización dependiendo el proceso al que corresponda.

**5.2.2 Análisis de gestión de riesgo.** En esta etapa se realizará un inventario de los activos de la compañía, a los cuales se les asignará una puntuación para valorar las amenazas, salvaguardas, estimar los riesgos y el impacto que dichas amenazas producen sobre cada uno de los activos.

El análisis de riesgos es una aproximación para determinar el riesgo siguiendo unos pasos definidos:

- ✓ Determinar los activos relevantes para la organización, su interrelación con los diferentes procesos y su valor, en el sentido de impacto (costos).
- ✓ Determinar a qué amenazas están expuestos aquellos activos.
- ✓ Determinar qué salvaguardas están implementadas y que tan eficaces son frente al riesgo.
- ✓ Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- ✓ Estimar el riesgo, definido como el impacto contenido con el índice de ocurrencia (o expectativa de materialización) de la amenaza.






**5.2.3 Identificación de activos.** Para realizar la identificación de los activos se contó con la colaboración de las personas encargadas y las cuales nos brindaron la información necesaria.

A continuación en la **¡Error! No se encuentra el origen de la referencia.** REF \_Ref449085116 \h \\* MERGEFORMAT **¡Error! No se encuentra el origen de la referencia.**, se encuentra la lista de los activos a los cuales se les realizará el estudio del entorno de seguridad de la compañía PINZÓN PINZÓN & ASOCIADOS, la tabla está compuesta por la cantidad de cada uno de los activos, adicional el nombre de cada activo y por último los aplicativos que allí se almacenan o de alguna manera están inmersos en estos.

Estos activos hacen referencia únicamente al área de TI, ya que este es el alcance del proyecto.

Cuadro 2 Identificación de Activos

Cantidad	Activos	Aplicativos
1	HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red). 	HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red). Pfsense 6.1( FreeBSD) Proxy, Firewall y VPN
1	HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red). 	HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red). ( Centos 6.5) Asterisk Puro (Planta telefónica)
1	Servidor HP ProLiant ML10 v2 (Ram 8 GB, 4 DD 1 TB en RAID 10, 2 tarjetas de red, Procesador Xenon) 	Servidor HP ProLiant ML10 v2 (Ram 8 GB, 4 DD 1 TB en RAID 10, 2 tarjetas de red, Procesador Xenon) Centos 6.5 a. Servidor de archivos ( Samba), Archivos b. Servidor de BD (Mysql) , CRM c. Fenix Data Web (Servidor web Apache ),Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión d. Fax Server
2	Equipos de TI	Disco Duro Externo 500 Gb Backup
1		Disco duro de 1Tb
2		UPS 600 Kba
1		Gateway 4 FXO GrandStream
2		Gateway 8 FXO GrandStream
1		DVR 16 Cámaras 2 TB
1		Biométrico de Acceso
1		Router Cisco WIFI
12		Equipos Portátiles
12		Equipos de escritorio
1		Red Local
25		Licencias de Antivirus
1	Infraestructura	Instalaciones de la empresa
5	Recurso Humano	Operadores de centro de TI
1	Seguridad Física	Vigilancia

Fuente: Autores proyecto.

**5.2.4 Reporte de vulnerabilidades.** En el **Anexo C**, se encontrará un reporte de vulnerabilidades, luego de realizar una evaluación a los diferentes servidores de la compañía PINZÓN PINZÓN & ASOCIADOS, reporte que ayudó a verificar las diferentes vulnerabilidades que se encontraron en conjunto con los otros documentos y análisis que se realizaron. Este reporte en concreto muestra las vulnerabilidades en las aplicaciones que se utilizan en la operación diaria para esta compañía y los servidores donde se alojan dichos desarrollos, este análisis se realizó enfocado a los servidores web y los servicios que allí se prestan, adicional a la información que esta almacenada en estos.

Cuadro 3 Reporte de Vulnerabilidades

Equipo	Vulnerabilidades
Servidor WEB	Servicios y puertos abiertos
	Las contraseñas no se cambian con periodicidad
	No hay políticas de contraseñas
	XSS y SQLinjection
	Interceptación de datos
	Problemas en la configuración del servicio Web local
	No existe un procedimiento o metodología para actualizar los desarrollos en producción
	No hay una metodología para el desarrollo seguro en aplicaciones
	El entorno de pruebas está en el mismo servidor de producción
	No hay planes de contingencia
	Los backups no son revisados
	El S.O. y los servicios están desactualizados.
Servidor Firewall y VPN	XSS y SQLinjection
	No hay políticas de contraseñas
	No hay planes de contingencia
	Los backups no son revisados
	El S.O. y los servicios están desactualizados.
Servidor PBX	Problemas en la configuración del servicio Web local
	Servicios y puertos abiertos
	No hay políticas de contraseñas
	XSS y SQLinjection
	Interceptación de datos
	No hay planes de contingencia
	Los backups no son revisados
	El S.O. y los servicios están desactualizados.

Fuente: Autores del Proyecto.

Cuadro 4 Sugerencias para las vulnerabilidades encontradas

Equipo	Actividad
Servidor WEB	Desinstalar de paquetes e inhabilitar puertos
	Cambiar periódicamente la contraseña del Acceso Remoto al Sistema
	Implementar políticas de contraseñas
	Implementar Mod Securtiy
	Implementar cifrado de datos para todas sus aplicaciones
	Ajustar la configuración del servicio Web local
	Ajustar los desarrollos en producción a las mejores practicas
	Establecer mejores prácticas en los desarrollos seguros de sus aplicaciones
	Establecer un entorno de pruebas diferente al servidor de producción
	Diseñar el plan de contingencia
	Ejecutar y revisar los planes de contingencia
	Mantener actualizados los servicios
Servidor Firewall y VPN	Mod Securtiy
	Implementar políticas de contraseñas
	Diseñar el plan de contingencia
	Ejecutar y revisar los planes de contingencia
	Mantener actualizados los servicios
Servidor PBX	Ajustar la configuración del servicio Web local
	Desinstalar de paquetes e inhabilitar puertos
	Implementar políticas de contraseñas
	Implementar Mod Securtiy
	Implementar cifrado de datos para todas sus aplicaciones
	Diseñar el plan de contingencia
	Ejecutar y revisar los planes de contingencia
	Mantener actualizados los servicios

Fuente: Autores del Proyecto.

**5.2.5 Valoración de activos.** Las valoraciones para escala cualitativa de Activos serán las siguientes de acuerdo a la utilidad y servicio de cada una, cada una de las características evaluadas se enfocaron en los tres pilares de la seguridad como son: disponibilidad, confidencialidad, integridad y reposición, para lo cual se realizó el promedio de las mismas.

La tabla valorativa de riesgos se realizó de acuerdo a los diferentes activos que se evaluaron para la compañía, adicional se tuvo en cuenta la criticidad de los mismos y que valor podía llegar a tener y cómo se podía evaluar.

En la Cuadro 5 Escala Valorativa de Riesgos (Disponibilidad), se realiza una escala para poder evaluar la disponibilidad en cada uno de los activos, esto basado en el tiempo tolerable fuera de servicio en días.

Cuadro 5 Escala Valorativa de Riesgos (Disponibilidad)

DISPONIBILIDAD			
Descripción	Símbolo	Valor	Tiempo tolerable fuera de servicio
Muy Alta	MA	5	1 día
Alta	A	4	2 días
Media	M	3	3 días
Baja	B	2	4 días
Muy Baja	MB	1	5 días o más
Fuente: Autores Proyecto			

Fuente: Autores Proyecto.

En el Cuadro 6 Valoración de Riesgos (Integridad), la valoración es enfocada a la integridad de la información y por último en el Cuadro 7 Valoración de Riesgos (Confidencialidad), esta valoración es acerca de la confidencialidad de la misma, las cuales se muestra a continuación:

Cuadro 6 Valoración de Riesgos (Integridad)

INTEGRIDAD			
Descripción	Símbolo	Valor	Escala
Muy Alta	MA	5	Toda la información destruida
Alta	A	4	Gran cantidad de información importante dañada
Media	M	3	Gran cantidad de información dañada
Baja	B	2	Mínima información importante dañada
Muy Baja	MB	1	Mínima información dañada
Fuente: Autores Proyecto			

Cuadro 7 Valoración de Riesgos (Confidencialidad)

CONFIDENCIALIDAD			
Descripción	Símbolo	Valor	Tipo de Información
Muy Alta	MA	5	Toda la información revelada
Alta	A	4	Importante cantidad de información revelada
Media	M	3	Importante Cantidad de información no sensible revelada
Baja	B	2	Información revelada mínima
Muy Baja	MB	1	Información revelada mínima y no sensible
Fuente: Autores Proyecto			

Tabla 1 Valoración de los Activos

Aplicativos	Disponibilidad	Confidencialidad	Integridad	Reposición	Promedio
HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red).	5	3	3	3	3,5
Pfsense 6.1( FreeBSD) Proxy, Firewall y VPN	5	3	3	2	3,25
HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red).	3	3	3	3	3
( Centos 6.5)	3	3	3	2	2,75
Asterisk Puro (Planta telefónica)	3	3	3	3	3
Servidor HP ProLiant ML10 v2 (Ram 8 GB, 4 DD 1 TB en RAID 10, 2 tarjetas de red, Procesador Xenon)	5	3	3	5	4
Centos 6.5	5	5	5	2	4,25
a. Servidor de archivos (Samba), Archivos	4	4	4	5	4,25
b. Servidor de BD (Mysql) , CRM	5	5	5	5	5
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	5	5	5	5	5
d. Fax Server	2	2	2	1	1,75
Disco Duro Externo 500 Gb Backup	5	5	5	1	4
Disco duro de 1Tb	5	5	5	1	4
UPS 600 Kba	5	1	1	2	2,25
Gateway 4 FXO GrandStream	2	2	2	2	2
Gateway 8 FXO GrandStream	2	2	2	2	2
DVR 16 Cámaras 2 TB	3	4	3	2	3
Biométrico de Acceso	5	1	3	2	2,75

Tabla 1 Valoración de los Activos

Aplicativos	Disponibilidad	Confidencialidad	Integridad	Reposición	Promedio
Router Cisco WIFI	3	4	4	2	3,25
Equipos Portátiles	4	4	4	3	3,75
Equipos de escritorio	4	4	4	3	3,75
Red Local	5	1	1	2	2,25
Licencias de Antivirus	5	5	5	2	4,25
Instalaciones de la empresa	5	5	5	3	4,5
Operadores de centro de TI	4	5	5	3	4,25
Vigilancia	5	5	5	1	4

Fuente: Autores del proyecto

Luego de realizar la valoración de los activos teniendo en cuenta la valoración de la disponibilidad, la confidencialidad e integridad, se encontraron 11 activos que podrían tener inconvenientes de acuerdo al nivel establecido ya que el promedio de estos esta sobre 4, lo cual para la compañía es crítico para su operación y continuidad, así como para las leyes que rigen la compañía en cuanto a la confidencialidad de la información, la cual es crítica y es por la cual se debe velar.



**5.2.6 Amenazas.** Las amenazas identificadas en términos de seguridad y disponibilidad del servicio del área de TI, de la compañía PINZÓN, PINZÓN & ASOCIADOS, para los activos recolectados se dan a conocer en el Cuadro 8 Listado de Amenazas, a continuación:

Cuadro 8 Listado de Amenazas

Aplicativos y Activos	# ID	Amenazas
Instalaciones de la empresa	1	Seguridad TI
a. Servidor de archivos ( Samba), Archivos	2	Acceso a información no debida
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	3	Acceso a información no debida
Disco Duro Externo 500 Gb Backup Y Disco duro de 1Tb	4	Complejidad procedimiento Backup
Asterisk (Planta telefónica)	5	Sniffer
a. Servidor de archivos ( Samba), Archivos	6	Sniffer
b. Servidor de BD (Mysql) , CRM	7	Sniffer
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	8	Sniffer
a. Servidor de archivos ( Samba), Archivos	9	Robo de información
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	10	Robo de información
UPS 600 Kba	11	Falla de Hardware
a. Servidor de archivos ( Samba), Archivos	12	Bugs en configuración
Biométrico de Acceso	13	Acceso no autorizado
Router Cisco WIFI	14	Acceso no autorizado
Equipos Portátiles y escritorio	15	Virus o troyanos
Instalaciones de la empresa	16	Incendio
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	17	Ataque SQL Injection y XSS

Fuente: Autores del proyecto

**5.2.7 Valoración del impacto, probabilidad de ocurrencia.** Las valoraciones de los impactos que motivarán las amenazas identificadas para cada uno de los activos serán las siguientes de acuerdo a la vulneración de la seguridad del servicio de cada una.

Cuadro 9 Escala valorativa del impacto y Probabilidad de Ocurrencia

Valores	Valor Cualitativo	Impacto	Probabilidad
5	MA	Impacto Muy Alto/Muy Grave o Severo para la Organización	Muy alta
4	A	Impacto Alto/Grave para la Organización	Alta
3	MD	Impacto Medio/Moderado/Importante para la Organización	Media
2	B	Impacto Bajo/Menor para la Organización	Baja
1	MB	Impacto Muy Bajo/Irrelevante para la Organización	Muy baja

Fuente: Autores del Proyecto.

Se valorará bajo los siguientes parámetros:

- ✓ **Costos de reposición:** adquisición e instalación del activo más el costo de mano de obra (especializada) invertida en recuperar el valor del activo.
- ✓ **Capacidad de operar:** confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
- ✓ Sanciones por incumplimiento de la ley u obligaciones contractuales.

Cuadro 10 Escala Impacto

IMPACTO			
Descripción	Símbolo	Valor	Escala
Muy Alta	MA	5	Costos 10.000.000 o más
Alta	A	4	Costos entre 5.000.001 y 10.000.000
Media	M	3	Costos entre 1.000.001 y 5.000.001
Baja	B	2	Costos entre 300.001 y 1.000.000
Muy Baja	MB	1	Costos entre 10.000 y 300.000
Fuente: Autores Proyecto			

Tabla 2 Valoración del impacto y Probabilidad de Ocurrencia

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red).	1	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MD	MB	BA	3	1	2	2,0	2,0	
	2	Cortes eléctricos	Falta de UPS, planta eléctrica, daño de equipos	MB	MB	BA	1	1	2	1,3	1,8	
Pfsense 6.1 (FreeBSD) Proxy, Firewall y VPN	3	Código Malicioso	Falla de antivirus o falta de antivirus y control en las políticas de gestión de software	MB	MB	MB	1	1	1	1,0	1,0	
	4	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	MD	BA	MB	3	2	1	2,0	1,3	
	5	Paso de Virus	Propagación interna de virus	MB	MB	MB	1	1	1	1,0	1,0	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvagu	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
<b><u>HP ProLiant MicroServer Gen8 (Ram 4Gb, 1 DD 1TB, 3 Tarjetas de red).</u></b>	6	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MB	MB	BA	1	1	2	1,3	1,8	
	7	Cortes eléctricos	Falta de UPS, planta eléctrica, daño de equipos	MB	MB	BA	1	1	2	1,3	1,8	
S.O. ( Centos 6.5)	8	Bugs del Sistema Operativo	Falta de actualización del SO o la versión es antigua y toca instalar una nueva	BA	MB	BA	2	1	2	1,5	1,9	
	9	Falla de Software	Mala configuración del equipo	BA	BA	BA	2	2	2	2,0	2,0	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	10	Código Malicioso	Falla de antivirus o falta de antivirus y control en las políticas de gestión de software	MB	MB	BA	1	1	2	1,3	1,8	
Asterisk (Planta telefónica)	11	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	MD	BA	BA	3	2	2	2,3	2,1	Disponibilidad
	12	Robo de llamadas	Revisión de la políticas de seguridad e implementación de cifrado	MD	MB	BA	3	1	2	2,0	2,0	
	13	Bugs en configuración	Falta de actualización del SO o la versión es antigua y toca instalar una nueva	MD	BA	BA	3	2	2	2,3	2,1	Confidencialidad, Integridad y Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	14	Sniffer	Falta de cifrado de información	MA	A	MD	5	4	3	4,0	3,3	Confidencialidad, Integridad y Disponibilidad
<b>Servidor HP ProLiant ML10 v2 (Ram 8 GB, 4 DD 1 TB en RAID 10, 2 tarjetas de red, Procesador Xenon)</b>	15	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MA	MB	MD	5	1	3	3,0	3,0	Disponibilidad
	16	Cortes eléctricos	Falta de UPS, planta eléctrica, daño de equipos	MD	MB	MD	3	1	3	2,3	2,8	Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
S.O. Centos 6.5	17	Bugs del Sistema Operativo	Falta de actualización del SO o la versión es antigua y toca instalar una nueva	MD	MD	MB	3	3	1	2,3	1,3	
	18	Falla de Software	Mala configuración del equipo	MD	MD	MD	3	3	3	3,0	3,0	Disponibilidad
	19	Código Malicioso	Falla de antivirus o falta de antivirus y control en las políticas de gestión de software	MD	MB	MB	3	1	1	1,7	1,2	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
a. Servidor de archivos (Samba), Archivos	20	Robo de información	Falta de idoneidad en el personal contratado (fijo, temporal o contratista), falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de la información	A	A	A	4	4	4	4,0	4,0	Confidencialidad
	21	Acceso a información no debida	Falta de mantenimiento a las políticas de credenciales	A	A	A	4	4	4	4,0	4,0	Confidencialidad, Integridad y Disponibilidad
	22	Espacio en Disco	Falta de espacio en disco para el funcionamiento y para logs de auditoria	MB	MB	MB	1	1	1	1,0	1,0	



Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	23	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	BA	BA	MD	2	2	3	2,3	2,8	Disponibilidad
	24	Virus	Falla de antivirus o falta de antivirus y control en las políticas de gestión de software	BA	BA	BA	2	2	2	2,0	2,0	
	25	Bugs en configuración	Falta de revisión y auditoría en la configuración del servicio	A	A	MD	4	4	3	3,7	3,2	Confidencialidad, Integridad y Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	26	Sniffer	Falta de cifrado de información	MA	A	MD	5	4	3	4,0	3,3	Confidencialidad, Integridad y Disponibilidad
b. Servidor de BD (Mysql) , CRM	27	Robo de información	Falta de idoneidad en el personal contratado ( fijo, temporal o contratista), falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de la información	BA	MB	MD	2	1	3	2,0	2,8	Confidencialidad, Integridad y Disponibilidad
	28	Acceso a información no debida	Falta de mantenimiento a las políticas de credenciales	BA	MB	MD	2	1	3	2,0	2,8	Confidencialidad, Integridad y Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	29	Espacio en Disco	Falta de espacio en disco para el funcionamiento y para logs de auditoria	MB	MB	MB	1	1	1	1,0	1,0	
	30	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	MD	MB	MB	3	1	1	1,7	1,2	
	31	Bugs en configuración	Falta de revisión y auditoria en la configuración del servicio	BA	BA	BA	2	2	2	2,0	2,0	
	32	Sniffer	Falta de cifrado de información	MA	A	MD	5	4	3	4,0	3,3	Confidencialidad, Integridad y Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	33	Robo de información	Falta de idoneidad en el personal contratado (fijo, temporal o contratista), falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de la información	A	A	A	4	4	4	4,0	4,0	Confidencialidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	34	Acceso a información no debida	Falta de mantenimiento a las políticas de credenciales	A	A	A	4	4	4	4,0	4,0	Confidencialidad, Integridad y Disponibilidad
	35	Espacio en Disco	Falta de espacio en disco para el funcionamiento y para logs de auditoria	MB	MB	MB	1	1	1	1,0	1,0	
	36	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	MA	BA	BA	5	2	2	3,0	2,3	Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguada	Impacto	Probabilidad	Salvaguada	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	37	Lentitud	Falla en la configuración de los servicios y mantenimiento de la aplicación	BA	MB	MB	2	1	1	1,3	1,1	
	38	Bugs en configuración	Falta de revisión y auditoria en la configuración de la aplicación	BA	MB	BA	2	1	2	1,7	1,9	
	39	Ataque SQL Injection y XSS	Falta de implementación de seguridad de aplicaciones	MA	A	MA	5	4	5	4,7	4,9	Confidencialidad, Integridad y Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	40	Sniffer	Falta de cifrado de información	MA	A	MD	5	4	3	4,0	3,3	Confidencialidad, Integridad y Disponibilidad
d. Fax Server	41	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MB	BA	MB	1	2	1	1,3	1,1	
	42	Bugs en configuración	Falta de revisión y auditoría en la configuración del servicio	MB	MB	MB	1	1	1	1,0	1,0	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	43	Espacio en Disco	Falta de espacio en disco para el funcionamiento y para logs de auditoria	MB	MB	MB	1	1	1	1,0	1,0	
<b><u>Disco Duro Externo 500 Gb Backup Y Disco duro de 1Tb</u></b>	44	Falla de Hardware	Daño por desgaste o defectos de fabricación	BA	BA	BA	2	2	2	2,0	2,0	
	45	Complejidad procedimiento Backup	No se realice el Backup	A	MA	MA	4	5	5	4,7	4,9	Confidencialidad, Integridad y Disponibilidad



Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	46	Extravío	Falta de gestión de las políticas de seguridad	MA	BA	BA	5	2	2	3,0	2,3	Confidencialidad, Integridad y Disponibilidad
<b><u>UPS 600 Kba</u></b>	47	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MA	MD	A	5	3	4	4,0	4,0	Disponibilidad
<b><u>Gateway 4 FXO GrandStream y Gateway 8 FXO GrandStream</u></b>	48	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MD	BA	BA	3	2	2	2,3	2,1	Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	49	Caída del Servicio	Ataque al equipo, errores de configuración, defecto del equipo	BA	MB	MB	2	1	1	1,3	1,1	
	50	Errores de Software	Falta de actualización	BA	MB	BA	2	1	2	1,7	1,9	
	51	Bugs en configuración	Falta de revisión y auditoría en la configuración del servicio	MD	MB	MD	3	1	3	2,3	2,8	Confidencialidad, Integridad y Disponibilidad
<b>DVR 16 Cámaras 2 TB</b>	52	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	BA	BA	BA	2	2	2	2,0	2,0	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	53	Cortes eléctricos	Falta de UPS, planta eléctrica, daño de equipos	BA	MB	BA	2	1	2	1,7	1,9	
	54	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	BA	MB	BA	2	1	2	1,7	1,9	
	55	Errores de Software	Falta de actualización	MB	MB	BA	1	1	2	1,3	1,8	
	56	Bugs en configuración	Falta de revisión y auditoría en la configuración del servicio	MB	MB	BA	1	1	2	1,3	1,8	
<b><u>Biométrico de Acceso</u></b>	57	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	A	BA	MB	4	2	1	2,3	1,3	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	58	Acceso no autorizado	Falta de mantenimiento a las políticas de credenciales	MA	MD	A	5	3	4	4,0	4,0	Confidencialidad, Integridad y Disponibilidad
	59	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	A	MB	BA	4	1	2	2,3	2,1	Disponibilidad
	60	Falla de Software	Mala configuración del equipo	BA	MB	MB	2	1	1	1,3	1,1	
<b><u>Router Cisco WIFI</u></b>	61	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MB	MB	MB	1	1	1	1,0	1,0	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	62	Acceso no autorizado	Falta de mantenimiento a las políticas de credenciales	MA	MD	MA	5	3	5	4,3	4,8	Confidencialidad, Integridad y Disponibilidad
	63	Caída del Servicio	Ataque al servidor o falta de mantenimiento, disco lleno	MB	MB	MB	1	1	1	1,0	1,0	
	64	Errores de Software	Falta de actualización	MB	MB	MB	1	1	1	1,0	1,0	
	65	Cortes eléctricos	Falta de UPS, planta eléctrica, daño de equipos	MB	MB	MB	1	1	1	1,0	1,0	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
<b>Equipos Portátiles y escritorio</b>	66	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	BA	BA	BA	2	2	2	2,0	2,0	
	67	Falla de Software	Mala configuración del equipo	BA	BA	BA	2	2	2	2,0	2,0	
	68	Virus o troyanos	Falla de antivirus o falta de antivirus y control en las políticas de gestión de software	MA	MD	BA	5	3	2	3,3	2,3	Confidencialidad, Integridad y Disponibilidad
	69	Acceso a información no debida	Falta de mantenimiento a las políticas de credenciales	A	MD	BA	4	3	2	3,0	2,3	Confidencialidad, Integridad y Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguada	Impacto	Probabilidad	Salvaguada	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
<b><u>Red Local</u></b>	70	Falla de Hardware	Falta de mantenimiento, daño por desgaste o defectos de fabricación	MA	MB	MB	5	1	1	2,3	1,3	
	71	Cortes eléctricos	Falta de UPS, planta eléctrica, daño de equipos	MB	MB	MB	1	1	1	1,0	1,0	
	72	Acceso no autorizado	Falta de mantenimiento a las políticas de credenciales	MB	MB	MB	1	1	1	1,0	1,0	
<b><u>licencias de Antivirus</u></b>	73	Caducidad de las licencias	Falta de adquisición o renovación	MA	MB	BA	5	1	2	2,7	2,2	Confidencialidad e Integridad
	74	Falla de Software	Mala configuración del equipo	MB	MB	BA	1	1	2	1,3	1,8	

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
	75	Bugs en configuración	Falta de revisión y auditoría en la configuración del servicio	MD	MB	BA	3	1	2	2,0	2,0	
<b><u>Instalaciones de la empresa</u></b>	76	Incendio	Falta de extintores, planes de evacuación y capacitación	MD	BA	MA	3	2	5	3,3	4,6	Integridad y Disponibilidad
	77	Terremoto	Falta de un plan de evacuación y capacitación	MB	MB	MB	1	1	1	1,0	1,0	
	78	Terrorismo	Falta de un plan	MB	MB	MB	1	1	1	1,0	1,0	
	79	Seguridad TI	Destrucción, alteración, robo.	MA	MA	MA	5	5	5	5,0	5,0	Confidencialidad, Integridad y Disponibilidad



Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
<b><u>Operadores de centro de TI</u></b>	80	Ingeniería Social	Falta de charlas informativas referente a ingeniería social, como evitarlas	MD	MD	MD	3	3	3	3,0	3,0	Confidencialidad, Integridad y Disponibilidad
	81	Extorciones por información	Extracción de información confidencial	MA	MB	BA	5	1	2	2,7	2,2	Confidencialidad, Integridad y Disponibilidad
	82	Robo de información	Falta de idoneidad en el personal contratado (fijo, temporal o contratista), falta de mantenimiento de las políticas de seguridad en credenciales y	MA	MB	MD	5	1	3	3,0	3,0	Confidencialidad, Integridad y Disponibilidad

Aplicativos y Activos	# Riesgo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Salvaguarda	Impacto	Probabilidad	Salvaguarda	Riesgo Intrínseco	Riesgo Efectivo	Criticidad
			cifrado de la información									
<b><u>Vigilancia</u></b>	83	Robo, extorción, terrorismos	Falta de idoneidad en el personal contratado (fijo, temporal o contratista), falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de la información	MA	BA	BA	5	2	2	3,0	2,3	Confidencialidad, Integridad y Disponibilidad

Fuente: Autores del proyecto

**5.2.8 Análisis GAP.** Se realizó un análisis GAP a la compañía PINZÓN PINZÓN & ASOCIADOS, esto con el fin de tener otro resultado de tal manera que se pueda determinar el riesgo al que está expuesta dicha compañía y de esta manera se pueda decidir que riesgos se evitan, transfieren, mitigan y aceptan.

A continuación se presenta el Cuadro 11 Valoración de la implementación por control, la información recolectada y con su resultado:

Cuadro 11 Valoración de la implementación por control

Escala	Valoración de la implementación (%)	Descripción
No aplica	N/A	No aplica
Inexistente	$0 > X < 20$	La Organización no ha reconocido que hay un problema a tratar.
Inicial	$20 > X < 40$	La organización ha reconocido que existe un problema y que hay que tratarlo, sin embargo, no hay procesos estandarizados.
Repetible	$40 > X < 60$	Los procesos y los controles siguen un patrón regular, sin embargo no están aprobados ni formalizados.
Definido	$60 > X < 80$	Los procesos y los controles se documentan, aprueban y se comunican. No se ha definido mecanismos de monitoreo.
Gestionado	$X > 80$	Los controles se monitorean y se miden, se toman acciones donde los procesos no estén funcionando eficientemente.

Fuente: Autores del proyecto

Tabla 3 Gobierno y Responsabilidades de seguridad de la Información

GOBIERNO Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN		
Control	Valoración de la implementación	Observación
La gerencia aprueba y apoya las actividades de seguridad de la información.	80%	
Se han definido, aprobado por la gerencia, publicado y comunicado a los colaboradores el conjunto de políticas de seguridad de la información.	10%	
Las políticas de seguridad de la información son revisadas a intervalos planeados o cuando cambios significantes ocurran.	10%	
Las responsabilidades de seguridad de la información son definidas y asignadas.	50%	La responsabilidad recae sobre el Ingeniero de soporte, que fuera de hacer su labor, identifica algunos problemas de este tipo.
Se tiene contactos con autoridades relevantes	10%	
Se tiene contacto con grupos de interés especial, foros de seguridad y asociaciones de profesionales	10%	
La infraestructura de seguridad (documenta, técnica, física) es revisada a intervalos planeados o cuando cambios significativos ocurran	20%	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>27%</b>

Fuente: Autores del proyecto

Evaluando el gobierno y su responsabilidad en la seguridad de la información se ve reflejado en la *Tabla 3* Gobierno y Responsabilidades de seguridad de la Información, que aunque se cuenta con el apoyo de la alta gerencia aún no se han construido, comunicado e implementado las políticas de seguridad necesarias, ni roles y responsabilidades con el fin de salvaguardar la información. Por lo tanto el dominio de este tema es del 27%.

Tabla 4 Recursos Humanos

RECURSOS HUMANOS		
Control	Valoración de la implementación	Observación
Durante el proceso de contratación se verifican los antecedentes de los candidatos o contratistas, teniendo en cuenta la clasificación de la información la cual accederán.	70%	
Se mantiene acuerdos con los empleados y contratistas sobre el cumplimiento de los requerimientos de seguridad de la información.	40%	
Los empleados de la organización y cuando sea pertinente y los contratistas reciben formación adecuada en seguridad de la información.	20%	
Las responsabilidades y obligaciones en cuanto a seguridad de la información permanecen vigentes después de la terminación o cambio de funciones del contrato laboral.	10%	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>35%</b>

Fuente: Autores del proyecto.

En la evaluación en la parte de recursos humanos no se tienen establecidas las obligaciones y responsabilidades dentro del contrato laboral en todo lo concerniente a la seguridad de la información y es muy poco el porcentaje que se hace a los temas de acuerdos entre contratistas para este tema. Por lo tanto el promedio de cumplimiento es del 35%.

Tabla 5 Gestión de Activos

GESTIÓN DE ACTIVOS		
Control	Valoración de la implementación	Observación
Existe un inventario de activos, en el cual se identifica el dueño.	80%	
Se mantienen y se comunican las reglas de uso aceptable de los activos.	60%	
Los activos de información son clasificados y etiquetados según su criticidad y relevancia para la organización.	60%	
Se tienen controles para la gestión de medios removibles.	30%	
Se tienen controles para la disposición segura de los activos de información.	30%	

GESTIÓN DE ACTIVOS		
Control	Valoración de la implementación	Observación
Se tienen controles para el traslado seguro de los activos de información.	10%	
PROMEDIO DE CUMPLIMIENTO DEL DOMINIO		45%

Fuente: Autores del proyecto

En cuanto a la gestión de activos en la Tabla 5 Gestión de Activos, la falencia que se tiene en los controles asignados para el traslado seguro de los activos de información ya que es básico.

Tabla 6 Control de Acceso

CONTROL DE ACCESO		
CONTROL	Valoración de la implementación	Observación
Se tienen controles para la asignación, bloqueo y modificación de accesos.	70%	
La asignación de información de autenticación es asignada a través de un proceso formal.	80%	
Los derechos de acceso son revisados periódicamente.	10%	
La asignación de accesos es basado en roles.	70%	
El sistema de administración de password es interactivo y asegura password de calidad.	10%	
PROMEDIO DE CUMPLIMIENTO DEL DOMINIO		48%

Fuente: Autores del proyecto.

En la *Tabla 6* Control de Acceso, se realiza la evaluación de control de acceso en la cual se evidencia que no se tiene establecida una revisión periódica de los permisos, así como no se tiene establecidas políticas para las contraseñas seguras.

En el tema de control de cifrado se evidencia en la *Tabla 7* Control de Cifrado, que tan solo existe el 10% de cumplimiento ya que no se tienen los controles suficientes antes este tema.

Tabla 7 Control de Cifrado

CONTROL DE CIFRADO		
Control	Valoración de la implementación	Observación
Se han definido controles de cifrado para proteger la información sensible.	10%	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>10%</b>

Fuente: Autores del proyecto.

En la *Tabla 8* Seguridad Física, se evalúa la seguridad física, donde encontramos falencias en la definición de perímetros de seguridad establecidos en las áreas donde se almacena o procesa información crítica, adicional no se tienen los suficientes controles para trabajar en dichas áreas. No se tiene un plan de respaldo ante cualquier eventualidad de desastre y es muy poco el respaldo que se tiene ante eventualidades como cortes de energía eléctrica.

Tabla 8 Seguridad Física

SEGURIDAD FÍSICA		
Control	Valoración de la implementación	Observación
Se han definido los perímetros de seguridad de las áreas donde se almacena o procesa información crítica o sensible.	10%	
Las áreas se han protegido con controles de acceso apropiados.	20%	
Se han definido y aplicado controles para trabajar en áreas seguras.	10%	
Se ha diseñado y aplicado protección física contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural.	10%	
Los equipos están protegidos contra fallas en el suministro de energía.	30%	
El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información está protegidos contra interceptaciones o daños.	20%	
Planea y desarrolla el programa de mantenimiento.	20%	
Los equipos desatendidos se les dan la protección adecuada.	20%	
Se definió, aprobó publicó y comunicó la política de escritorio y pantalla despejada.	90%	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>26%</b>

Fuente: Autores del proyecto.

En cuanto a la seguridad de las operaciones se refleja que las actividades del administrador y el operador del sistema no son registradas y los logs no son protegidos y revisados regularmente, adicional no se cuenta con controles suficientes para la no instalación de software permitido por la compañía, ni controles para temas de dispositivos móviles, todo esto se encuentra en la *Tabla 9 Seguridad en Operaciones*.

Tabla 9 Seguridad en Operaciones

<b>SEGURIDAD EN LAS OPERACIONES</b>		
<b>Control</b>	<b>Valoración de la implementación</b>	<b>Observación</b>
Los procedimientos de operación se documentan, mantienen y están disponibles para todos los usuarios que los necesiten.	<b>70%</b>	
Se controlan los cambios en los servicios y los sistemas de procesamiento de información.	<b>30%</b>	
Los ambientes de desarrollo, pruebas y producción están separados con el fin de reducir el riesgo de accesos o cambios no autorizados en el ambiente de producción	<b>70%</b>	
Se tienen controles de detección, prevención de malware.	<b>95%</b>	
Se realizan copias de respaldo de la información y se realizan pruebas de restauración periódicas.	<b>40%</b>	
Los logs de los sistemas mantenidos y revisados regularmente.	<b>30%</b>	
Las actividades del administrador y el operador del sistema son registrados y los logs son protegidos y revisados regularmente.	<b>5%</b>	
Los relojes de todos los sistemas de procesamiento de información están sincronizados con una fuente de tiempo exacta y acordada.	<b>10%</b>	
Se han definido, aprobado e implementado controles para la instalación de software en los sistemas operativos	<b>10%</b>	
Se han definido controles para mitigar el riesgos de uso de dispositivos móviles	<b>20%</b>	
Se han definido controles para el teletrabajo.	<b>95%</b>	
Se obtiene información oportuna sobre las vulnerabilidades técnicas de los sistemas de información, se evalúa la exposición de la organización a dichas vulnerabilidades y se toman acciones apropiadas para tratar los riesgos asociados	<b>60%</b>	
Se restringe y controla el uso de programas utilitarios.	<b>20%</b>	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>43%</b>

Fuente: Autores del Proyecto.



En la seguridad en las comunicaciones el porcentaje más bajo se encontró en la protección de la mensajería electrónica como el correo entre otros, adicional no se cuenta con controles necesarios para monitorear y salvaguardar la red y lo que viaja por ella, esto se muestra a continuación en la Tabla 10 Seguridad en las Comunicaciones.

Tabla 10 Seguridad en las Comunicaciones

<b>SEGURIDAD EN LAS COMUNICACIONES</b>		
<b>Control</b>	<b>Valoración de la implementación</b>	<b>Observación</b>
Se controla y monitorea el acceso a la red.	<b>30%</b>	
Niveles de servicio y requerimientos de gestión de todos los servicios de red son identificados e incluidos en los acuerdos de servicios de red.	<b>95%</b>	
Grupos de servicios de información, usuarios y sistemas de información son segregados.	<b>70%</b>	
Se han establecido acuerdos para el intercambio de la información entre la organización y partes externas	<b>N/A</b>	
La información contenida en la mensajería electrónica es protegida.	<b>20%</b>	
Se identifican, mantienen y revisan periódicamente los acuerdos de confidencialidad.	<b>70%</b>	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>48%</b>

Fuente: Autores del Proyecto.

En cuanto a la adquisición, desarrollo y mantenimiento de los sistemas de información se encontró que en promedio se cumple con un 50% de los criterios evaluados como se muestra en la Tabla 11 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información, donde las falencias que se encontraron están en no contar con documentos o reglas definidas para el desarrollo del software y no tener control sobre los cambios que se realizan en este.

Tabla 11 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

<b>ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN</b>		
<b>Control</b>	<b>Valoración de la implementación</b>	<b>Observación</b>
Se han definido y documentado reglas para el desarrollo de software.	<b>40%</b>	
La información involucrada en servicios transaccionales de aplicaciones es protegida.	<b>90%</b>	
Cambios a los sistemas dentro del ciclo de vida de desarrollo son controlados formalmente.	<b>40%</b>	
La organización establece y protege los ambientes de desarrollo.	<b>70%</b>	

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		
Control	Valoración de la implementación	Observación
La organización supervisa y monitorea el desarrollo de software contratado externamente.	N/A	
Se ejecutan pruebas de funcionalidad y de seguridad durante el desarrollo.	60%	
PROMEDIO DE CUMPLIMIENTO DEL DOMINIO		50%

Fuente: Autores del Proyecto.

En la relación con los proveedores se encontró que aún no se encuentran establecidos, ni documentados los procedimientos para el acceso a los proveedores, así como no se encuentran establecido el monitoreo y la auditoria a los servicios consumidos por los mismos, por lo tanto como se observa en la *Tabla 12 Relación con Proveedores*, solo se ha completado el 20% del cumplimiento en este ítem.

Tabla 12 Relación con Proveedores

RELACIÓN CON PROVEEDORES		
Control	Valoración de la implementación	Observación
Se han documentado los requerimientos de seguridad de la información para mitigar el riesgo asociado con el acceso de proveedores a los activos de la organización.	20%	Un proveedor puede ser un abogado que se conecta vía teletrabajo a la empresa para realizar determinadas labores para lo cual nunca se monitorea.
La organización regularmente monitorear, revisa y auditar los servicios entregados por proveedores.	20%	
PROMEDIO DE CUMPLIMIENTO DEL DOMINIO		20%

Fuente: Autores del Proyecto.

El tema de la gestión de incidentes también se encuentra en un 20% de cumplimiento ya que no se tienen establecidas las responsabilidades y los procedimientos para dar respuesta a los diferentes incidentes de seguridad, así como no se tienen clasificados los mismos, como se muestra en la *Tabla 13* Gestión de los incidentes de seguridad de la Información.

Tabla 13 Gestión de los incidentes de seguridad de la Información

<b>GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>		
<b>Control</b>	<b>Valoración de la implementación</b>	<b>Observación</b>
Se han establecido las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información	20%	
Los eventos de seguridad de la información son evaluados y clasificados para determinar si son incidentes de seguridad de la información.	20%	
El conocimiento adquirido del análisis y la resolución de incidentes de seguridad de la información es usado para reducir la probabilidad o el impacto de incidentes futuros.	20%	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>20%</b>

Fuente: Autores del proyecto.

Tabla 14 Aspectos de la Seguridad de la Información en la Gestión de Continuidad de Negocio

<b>ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO</b>		
<b>Control</b>	<b>Valoración de la implementación</b>	<b>Observación</b>
La organización debe establecer, documentar, implementar y mantener controles para asegurar el nivel requerido de continuidad de la seguridad de la información en situaciones adversas.	20%	
El plan de continuidad es revisado y probado a intervalos regulares con el fin de asegurar que son válidos y efectivos durante una situación adversa	20%	
Las instalaciones de procesamiento de información están implementadas con redundancia para cumplir con los requerimientos de disponibilidad	80%	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>40%</b>

Fuente: Autores del Proyecto.

Tabla 15 Cumplimiento

CUMPLIMIENTO		
Control	Valoración de la implementación	Observación
Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos están definidos y documentados.	60%	
Se garantiza la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes.	95%	
<b>PROMEDIO DE CUMPLIMIENTO DEL DOMINIO</b>		<b>78%</b>

Fuente: Autores del Proyecto

Tabla 16 Promedio General de Cumplimiento Análisis GAP

<b>PROMEDIO GENERAL</b>	<b>38%</b>
-------------------------	------------

Fuente: Autores del Proyecto.

Luego de realizar este análisis el promedio de cumplimiento se obtuvo como resultado un 38%, esto quiere decir según la *Tabla 16*, que la empresa se encuentra en una etapa inicial, se evidencia el respaldo de la dirección, pero es necesario definir una estrategia de seguridad de la información, la cual este alineada con la estrategia corporativa.

Se puede evidenciar luego de este análisis que aún no se han definido, aprobado y comunicado las políticas de seguridad que se deben establecer dentro de la compañía, teniendo en cuenta esto en la parte de recursos humanos no se tienen responsabilidades y obligaciones frente al cambio de funciones o terminación de contrato laboral en cuanto al impacto que esto pueda tener en temas de permisos a la información.

No se cuenta con los controles necesarios para trasladar de una manera segura los activos de información, adicional a esto no se cuenta con la revisión periódica de los permisos asignados a cada una de las personas que trabajan en la compañía, las contraseñas son muy inseguras puesto que no se tiene establecido una metodología para la creación y cambio de las mismas.

Los datos en los diferentes sistemas de información viajan de forma insegura ya que no se cuenta con ningún tipo de cifrado para proteger la información sensible de la compañía.

En cuanto a la seguridad física no se tiene establecido un perímetro o áreas sensibles, no se cuenta con los controles necesarios para salvaguardar los activos, no se cuenta con un plan de respaldo ante eventualidades como incendio, inundación entre otras.

En el tema de seguridad en las operaciones no se cuenta con los logs activos, esto con el fin de ser registrados los eventos, no se cuenta con una fuente de tiempo que sincronice los sistemas de información, tienen falencias en las políticas respecto a la instalación de software y el control de programas no útiles para la operación de la compañía.

No se cuenta con ningún control sobre la red para temas de monitoreo, la información contenida en el correo electrónico no está protegida de la mejor manera.

**5.2.9 Determinación del riesgo.** Contexto: Pinzón Pinzón & Asociados Abogados, Empresa del sector Jurídico, Asuntos Regulatorios, Derecho Empresa, Derecho Laboral, Litigios y Propiedad Intelectual.

En base al análisis realizado anteriormente, teniendo en cuentas los activos y de allí sus amenazas y vulnerabilidades dio como resultado la determinación final del riesgo, el cual se plasma en la Tabla 17 Determinación del riesgo, que se ve reflejado a continuación:

Tabla 17 Determinación del riesgo

NIVEL IMPACTO	RIESGO PURO			
<b>CATASTROFICO (100)</b>			4,5,6,7,8,17	1
<b>MAYOR (75)</b>		13	9,10,11	2,3
<b>MODERADO (50)</b>			12,14	
<b>MENOR (25)</b>	15,16			
	<b>IMPROBABLE (25)</b>	<b>POSIBLE(50)</b>	<b>PROBABLE(75)</b>	<b>CASI CERTEZA (100)</b>
	<b>PROBABILIDAD</b>			

Fuente: Autores del proyecto.

Tabla 18 Valoración del Riesgo

Aplicativos y Activos	# ID	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Promedio
Instalaciones de la empresa	1	Seguridad TI	Destrucción, alteración, robo.	100	100	100
Disco Duro Externo 500 Gb Backup Y Disco duro de 1Tb	4	Complejidad procedimiento backup	No se realice el Backup	100	75	87,5
Asterisk (Planta telefónica)	5	Sniffer	Falta de cifrado de información	100	75	87,5
a. Servidor de archivos (Samba), Archivos	6	Sniffer	Falta de cifrado de información	100	75	87,5
b. Servidor de BD (Mysql) , CRM	7	Sniffer	Falta de cifrado de información	100	75	87,5
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	8	Sniffer	Falta de cifrado de información	100	75	87,5
c. Fenix Data Web (Servidor web Apache), Clientes, Contactos, Control de tiempos, Seguimientos, Facturación y Gestión documental.	17	Ataque SQL Injection y XSS	Falta de implementación de seguridad de aplicaciones	100	75	87,5

Fuente: Autores del Proyecto

**5.2.10 Documento de declaración de aplicabilidad (SOA).** En el **Anexo C DOCUMENTO DE DECLARACIÓN DE APLICABILIDAD (SOA)**, se encontrará la información del análisis que se le realizó a la compañía PINZÓN PINZÓN & ASOCIADOS, en este documento se evidencian los controles que hasta el momento están siendo aplicados y otros los cuales salieron luego de realizar la determinación del riesgo, controles que se sugiere se deben poner en práctica de acuerdo a la capacidad de la compañía para aceptarlos, mitigarlos, transferirlos y evitarlos, esto con el fin de tener mayor seguridad en el área de TI y a la vez ir alineándose con la norma ISO 27001:2013.

Dentro de lo más destacado luego del levantamiento se muestra en el Cuadro 12 Análisis basados en SOA.

Cuadro 12 Análisis basados en SOA

Cláusula	Objetivo de Control/Control
Políticas de la seguridad de la Información	Revisión de las políticas para seguridad de la información
Organización de Seguridad de la Información	Política para dispositivos móviles
Seguridad de los recursos humanos	Toma de conciencia, educación y formación en la seguridad de la información
	Terminación o cambio de responsabilidades de empleo
Gestión de Activos	Gestión de medios de soporte removibles
	Disposición de los medios de soporte
	Transferencia de medios de soporte físicos
Control de acceso	Gestión de derechos de acceso privilegiado
	Gestión de información de autenticación secreta de usuarios
	Revisión de los derechos de acceso de usuarios
	Uso de información de autenticación secreta
	Sistema de gestión de contraseñas
Criptografía	Política sobre el uso de controles criptográficos
	Gestión de claves
Seguridad Física y Ambiental	Perímetro de seguridad física
	Controles físicos de entrada
	Seguridad de oficinas, salones e instalaciones
	Protección contra amenazas externas y ambientales

Cláusula	Objetivo de Control/Control
	Ubicación y protección de los equipos
	Seguridad de equipos y activos fuera del predio
	Equipos de usuario desatendido
Seguridad de las operaciones	Separación de los ambientes de desarrollo, pruebas, y operacionales
	Copias de respaldo de la información
	Registro de eventos
	Protección de la información de registro
	Registros del administrador y del operador
	Sincronización de relojes
	Instalación de software en sistemas operativos
	Gestión de las vulnerabilidades técnicas
	Restricciones sobre la instalación de software
	Controles sobre auditorías de sistemas de información
Seguridad de las comunicaciones	Políticas y procedimientos de transferencia de información
	Acuerdos sobre transferencia de información
Adquisición, desarrollo y mantenimiento de sistemas	Política de desarrollo seguro
	Procedimientos de control de cambios en sistemas
	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones
	Restricciones sobre cambios en los paquetes de software
	Principios de organización de sistemas seguros
	Ambiente de desarrollo seguro
	Pruebas de seguridad de sistemas
	Prueba de aceptación de sistemas
	Protección de datos de prueba
Relaciones con los proveedores	Política de seguridad de la información para las relaciones con proveedores
	Tratamiento de la seguridad dentro de los acuerdos con proveedores
	Cadena de suministro de



Cláusula	Objetivo de Control/Control
	tecnología de información y comunicación
	Seguimiento y revisión de los servicios de los proveedores
	Gestión de cambios a los servicios de los proveedores
Gestión de incidentes de seguridad de la información	Responsabilidades y procedimientos
	Informe de eventos de seguridad de la información
	Informe de debilidades de seguridad de la información
	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
	Respuesta a incidentes de seguridad de la información
	Aprendizaje obtenido de los incidentes de seguridad de la información
	Recolección de evidencia
Aspectos de seguridad de la información de la gestión de continuidad de negocio	Planificación de la continuidad de la seguridad de la información
	Implementación de la continuidad de la seguridad de la información
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	Disponibilidad de instalaciones de procesamiento de información.
Cumplimiento	Reglamentación de controles criptográficos
	Revisión independiente de la seguridad de la información
	Cumplimiento con las políticas y normas de seguridad
	Revisión del cumplimiento técnico

Fuente: Autores del Proyecto.

## 6. PLANES DE TRATAMIENTO

Ya que la base del funcionamiento del negocio de la entidad radica en uso de la información almacenada de sus clientes, diferentes procesos, por esta razón

el trabajo tendrá como objetivo mantener la disponibilidad, integridad y confidencialidad de la información, teniendo en cuenta los elementos que permiten el buen funcionamiento de los sistemas.

Luego de realizar el análisis de riesgos a la compañía PINZÓN PINZÓN & ASOCIADOS, se llegó a la conclusión que eran necesarios los siguientes planes de tratamiento, esto con el fin de mitigar el impacto que puede llegar a tener si las amenazas detectadas se materializan, por lo tanto son riesgos que la compañía no estaría dispuesta a asumir:

- ✓ Seguridad Física
- ✓ Políticas de Seguridad de Usuarios
- ✓ Políticas para realizar Backups
- ✓ Controles de Cifrado de la Información
- ✓ Políticas de contratación
- ✓ Políticas de monitoreo
- ✓ Seguridad en aplicaciones

## **6.1 PLAN DE TRATAMIENTO N° 1**

### **6.1.1 Seguridad física**

#### **Objetivo**

Tomar medidas de seguridad física para resguardar los elementos físicos de TI y robustecer la seguridad de la información.

#### **Alcance**

Recomendaciones para mitigar el riesgo latente que refiere a la seguridad física donde se encuentran ubicados los equipos de TI y por lo tanto la información de la compañía.

#### **Plan**

Luego de realizar el análisis de riesgos de la compañía PINZÓN PINZÓN & ASOCIADOS se recomienda para fortalecer la seguridad física:

1. Instalar una puerta, la cual tenga rejillas por el tema de ventilación ya que los equipos producen temperaturas altas.
2. Adecuar el rack de servidores de tal manera que se tenga refrigeración para los mismos y de esta forma mantener los equipos trabajando bajo un ambiente adecuado.
3. Para este punto 2, se recomienda realizar una inversión para la compra de un rack que cuente con refrigeración incorporada o comprar un sistema de refrigeración para el cuarto donde se encuentra la infraestructura de TI.
4. Tener una doble autenticación para el ingreso, si se tiene la posibilidad de instalar dicho artefacto.

## **6.2 PLAN DE TRATAMIENTO N° 2**

## **6.2.1 Políticas de seguridad de usuarios**

### **6.2.1.1 Política de control de acceso**

#### **Objetivo**

Crear procedimientos para la asignación de permisos y control de accesos a los usuarios.

#### **Alcance**

Permisos y control de acceso asignados a personal de TI a los sistemas informáticos de la compañía.

#### **Política**

El grupo de Seguridad Informática administrará el control de acceso a los diferentes sistemas de información de la compañía.

Se otorgarán permisos con requerimientos previos del superior y dichos permisos serán solicitados por medio de un formato previamente elaborado, todo usuario creado y asignado será personal e intransferible, por lo tanto debe llenarse un acta de compromiso de esto.

Todo permiso a los diferentes sistemas de bases de datos, sistemas operativos y acceso físico al centro de cómputo de la compañía será aprobado por el grupo de Seguridad Informática.

El grupo de seguridad informática debe realizar constantes mantenimientos de usuarios activos e inactivos, esto con el fin de evitar ingresos no autorizados a los diferentes sistemas de información.

#### **Perfiles de Usuarios**

Determinar perfiles de usuario según su responsabilidad y tareas asignadas dentro de la compañía, se sugiere crear los usuarios bajo los siguientes perfiles:

- Administrador
- Oficial de Seguridad
- Operador: Login de Usuarios de TI
- Lectura
- Updates: Usuarios aplicativos de sistemas.

#### **Política de Cuenta**

Se tiene grupos diferenciados con acceso a producción y los cuales se detallan a continuación:

## USUARIO SA

- Se cambiará este password cada mes.
- Los usuarios con características del SA pueden ser: El Administrador de la Base de datos, Seguridad Informática como Administrador de control de accesos a la base de datos y el Administrador del sistema central.

## USARIO DE CONSULTA / LECTURA

- El acceso de desarrollo será solamente de lectura.
- El usuario de consulta es para revisión de problemas.
- Deberán registrarse al horario de uso asignado.
- Deben conectarse solo por el tiempo necesario, no deberán mantener conexiones abiertas por largo tiempo, peor de un día al otro.
- Los permisos serán otorgados de acuerdo al grupo aplicativo que manejen.

## APLICATIVOS / ACTUALIZACIONES

- Usuarios creados para manejo interno en las aplicaciones
- Estos usuarios no deben ser conectados en equipos no autorizados (área de desarrollo)
- Los password de estos usuarios deben cumplir con la política de seguridad (cifrado).

## OPERADORES

- Por política sólo los operadores podrán sacar respaldos y restaurar.
- El usuario Operador para los procesos batch tendrá acceso con rol SA.
- El usuario operador es el único autorizado para compilación de programas

## ADMINISTRADORES DE BASE DE DATOS

- Por política realizará monitoreo de la base de datos
- No puede realizar consultas a información de la base
- Alertará sobre mal uso de los recursos de la base

## OFICIAL DE SEGURIDAD

- Realizará la creación y eliminación de usuarios.
- Asignación de permisos y seguimiento de usuarios.

## **Política de Password**

- Longitud del password: superior o igual a 8 caracteres.
- ...Contener la combinación de los siguientes puntos:

- Letras mayúsculas
- Letras minúsculas
- Números
- Símbolos
- ...Expiración de la clave: 90 días.
- ...Para administradores cambiará cada 30 días.
- ...El número de sesiones concurrentes de un mismo usuario es limitado.
- ...El usuario debe ser usado en el equipo personal a él asignado.
- ...El password es personal e intransferible.
- El password no puede ser igual al nombre de usuario o cualquier variación (al revés, mayúsculas, etc.), alias o sobrenombre de la persona.
- ...El password no puede contener palabras existentes en diccionarios sin importar el idioma.
- El password no puede usar patrones como secuencias de números o caracteres y cadenas repetidas.

Se le sugiere a la compañía que cada empleado tenga conocimiento de estas políticas, se adjunta formato para este fin el cual será encontrado en el **Anexo D**.

### **6.3 PLAN DE TRATAMIENTO N° 3**

#### **6.3.1 Políticas para realizar backups**

**Objetivo**

Realizar un manual de procedimientos donde se estipulen los pasos a seguir para realizar sus respectivos Backups y tener sitios determinados para almacenar dichos Backups.

**Alcance**

Roles, responsabilidades y acceso a la información respaldada en medios externos e internos.

**Políticas**

Para una correcta realización y seguridad de Backups se deberán tener en cuenta estos puntos:

1. Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder realizar una reinstalación en caso de sufrir un percance.
2. Se deben determinar los medios y herramientas correctos para realizar los Backups, teniendo en cuenta los espacios necesarios, tiempos de lectura/escritura, tipo de Backup a realizar, entre otros.
3. El almacenamiento de los Backups debe realizarse en lugares diferentes de donde reside la información principal. De este modo se evita la pérdida total si hay un desastre que afecte todas las instalaciones de la compañía.
4. Se debe verificar periódicamente la integridad de los Backups que se están almacenando, esto con el fin de asegurar que al momento de requerir restaurar alguno de ellos funcione como se espera.
5. Se debe contar con un procedimiento adecuado para garantizar la integridad física de los respaldos, en previsión de robo, destrucción o pérdida.
6. Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por lo tanto se recomienda cifrar dicha información para mayor seguridad.
7. Se debe de contar con un procedimiento previamente definido para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
8. Provisionar equipos de hardware con características similares a los utilizados para el proceso normal de la operación de la compañía, en condiciones necesarias para entrar en funcionamiento en caso de desastres físicos.

Puede optarse por:

- **Equipos Externos:** otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro ocurrido.
- **Equipos Internos:** equipos donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son respaldo del otro y están en disposición de ser usados en caso de emergencia.

Se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios, esto para tener un plan de contingencia y poner en práctica de alguna manera la continuidad del negocio.

### **Roles y Responsabilidades**

Determinar que roles de usuario según su responsabilidad y tareas asignadas dentro de la compañía, interviene dentro del proceso de los Backups:

- Administrador de Backups: Persona encargada de realizar los Backups.
- Transportador: Encargado de llevar los Backups fuera de las instalaciones de la compañía.
- Probador: Encargado de probar Backups cada cierto período de tiempo.

## **6.4 PLAN DE TRATAMIENTO N° 4**



#### **6.4.1 Controles de cifrado de la información**

Para los Controles de cifrado se utilizarán sistemas y técnicas de cifrado para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección asegurando los pilares de la seguridad como son la confidencialidad, integridad y disponibilidad.

##### **Política de Utilización de Controles de Cifrado**

Se utilizarían los controles de cifrado en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito de la compañía.
3. Para el resguardo de información.

#### **6.4.2 Cifrado**

##### **Políticas de Seguridad de la Información**

Mediante la evaluación de riesgos que se llevó a cabo el Propietario de la Información y el Oficial de Seguridad Informática, tomará la decisión de que nivel de protección es requerido, teniendo en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves de cifrado a utilizar.

Firma Digital Se tomarán recaudos para proteger la confidencialidad de las claves privadas. Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

#### **6.4.3 Administración de claves**

##### **Protección de Claves de Cifrado**

Se sugiere implementar un sistema de administración de claves de cifrado para respaldar su utilización por parte de los usuarios de la compañía. Todas las claves serán protegidas contra modificación y/o destrucción, las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada. Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

### **6.5 PLAN DE TRATAMIENTO N° 5**

### **6.5.1 Políticas de contratación – recursos humanos**

#### *Antes de la contratación*

En conjunto con el departamento de Recursos humanos, se debe asegurar que se está empleado un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar.

Se deben realizar comprobaciones de procedencia, formación, conocimientos, etc. Porcentaje de nuevos empleados, contratistas, consultores, temporales, etc., que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.

#### *Durante la contratación*

La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandona la organización.

Se debe asegurar que esto se documenta claramente en materiales de concienciación, contratos del empleado, etc., adicional contemplar la posibilidad de una revisión anual por parte del departamento de recursos humanos de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.

#### *Cese o cambio de puesto de trabajo*

El inventario de activos debe estar actualizado y verificado cada cierto periodo de tiempo esto con el fin de cuando un empleado deja la organización facilitar el empalme de los activos que esta persona tenía a su cargo.

Se debe tener un procedimiento previamente establecido para estos casos de tal manera que se pueda saber los diferentes accesos que la persona tenía a los diferentes sistemas de información y restringir dichos accesos a la información luego de no pertenecer a la compañía.

Tener identificadores de usuarios pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).

## **6.6 PLAN DE TRATAMIENTO N° 6**

## **6.6.1 Política de monitoreo de base de datos**

### **Objetivo**

Monitoreo del funcionamiento, rendimiento, mantenimiento y comportamiento de elementos de la infraestructura tecnológica.

Todo servicio que se brinda debe ser monitoreado y revisado para garantizar su funcionalidad.

Informes compartidos en file server, con acceso restringido. Definir responsable y periodicidad de entrega.

Informes mensuales: Plazo de entrega hasta 5 días hábiles del mes siguiente.

### **Monitoreo por elemento**

#### **INFRAESTRUCTURA**

- Recursos disponibles asignados
- Disponibilidad de servicios
- Revisión de estado de antivirus

#### **REDES:**

- Seguridad perimetral del IPS
- Uso de ancho de banda
- Uso de switch

#### **BASE DE DATOS:**

- Rendimiento de MySQL
- Espacio disponible de datos.

#### **SOPORTE:**

- Seguridad de correo
- Navegación y contenido (Internet).

### **Arquitectura**

Monitoreo de plataforma de integración

### **Responsabilidades**

- Líder de Grupo de Solución: Asegurar que se cumplan las actividades de monitoreo y entrega de informes.
- Subgerente responsable: Revisión de informes y determinar acciones a tomar.
- Revisor: Revisar disponibilidad de informes.
- Políticas de manejo de ambiente de Preproducción

### **General**

- El ambiente Preproducción no será utilizado para desarrollar aplicaciones, este ambiente está destinado para realizar pruebas de usuario final.

- Todas las aplicaciones existentes y nuevas con sus mejoras o cambios deben ser probadas en este ambiente Pre-producción, antes de instalarlas en el ambiente de Producción.
- La administración de este ambiente estará bajo la responsabilidad de Bases de Datos por el lado de Ingeniería, el jefe de desarrollo.
- En este ambiente no se ejecutará procesos de producción
- Se definirán un grupo de usuarios de consulta en este ambiente Pre-producción, los mismos que serán utilizados por los desarrolladores en la verificación de data resultado de las pruebas efectuadas por los usuarios finales.

#### **Responsabilidad de Administrador de Base de Datos**

- Crear un usuario operador con los accesos necesarios para realizar los pases. El buen uso del usuario operador es responsabilidad del administrador de desarrollo.
- Crear los usuarios aplicativos de lectura a la base.

#### **Responsabilidad de Desarrollo**

- Ejecutar los pases de desarrollo en dicho ambiente.
- Mantener la confidencialidad de la clave del usuario operador.

### **6.7 PLAN DE TRATAMIENTO N° 7**

### **6.7.1 Seguridad en aplicaciones**

#### **1. Asegurar red corporativa**

Asegurar, proteger y hacer cumplir las políticas consistentemente en todos los dispositivos de la red bien sea propiedad de la empresa o de los empleados. Con esto no sólo se tiene control en torno de las aplicaciones web a las que se accede desde los equipos de escritorio o portátiles, sino también desde dispositivos móviles.

#### **2. Extender la protección contra malware en dispositivos móviles**

Esta acción debe ser una prioridad; nunca hay que dejar los dispositivos móviles que tienen acceso a las aplicaciones de la red corporativa expuestos a amenazas potenciales. Los empleados deben ser conscientes que proteger los dispositivos móviles es fundamental, independientemente de quién es propietario del equipo.

#### **3. Establecer políticas contextualmente**

Tener un enfoque único para todos (genérico y ajustable), esto porque las necesidades y expectativas de los usuarios y de TI varían constantemente en el tiempo. Se deben aplicar las políticas de seguridad con base en el usuario, su ubicación, el dispositivo que están utilizando y la red.

#### **4. Reportar, ajustar y repetir**

Para mantener la seguridad de una manera efectiva y con controles de políticas adecuadas es esencial ajustar las políticas corporativas con base en los datos obtenidos en tiempo real de todos los usuarios y dispositivos. Utilizar las herramientas de reporte para entender no sólo cómo las políticas están impactando a los usuarios y su red, sino también para identificar y solucionar inconvenientes inmediatamente.

### **6.7.2 Firewall, IDS e IPS**

#### **1. Proteger la infraestructura con un firewall**

Se puede elegir entre firewalls de software o hardware para proteger los servidores. Se puede elegir entre varias ofertas de firewall que ofrece el mercado en este momento de acuerdo a las necesidades de la compañía.

#### **2. Asegurar que el firewall se está ejecutando**

Para que la infraestructura de TI y los servidores estén protegidos, el firewall

tiene que estar funcionando en todo momento, esto garantizará en un porcentaje alto la seguridad perimetral de la compañía.

### 3. Proteger la infraestructura con un WAF (Firewall para aplicaciones web)

Este firewall es dedicado para detener ataques dedicados a aplicaciones web, en el mercado existen muchas marcas y tipos de WAF, uno de los que se pudieron trabajar y es de acceso abierto es: ModSecurity: Open Source Web Application Firewall, esta implementación evitará ataques de: Cross site scripting (xss), sql injection, La Denegación de Servicio (DoS) o Denegación de Servicio Distribuida (DDoS), ataque de directorio lateral, entre otros.

### 4. Usar un sistema de detección de intrusos (IDS)

Existen diferentes soluciones y marcas para ejecutar un sistema de IDS basado en un host o red en función de sus necesidades y requisitos de cumplimiento.

### 5. Usar un sistema de prevención de intrusos (IPS)

Elegir un IPS que incluya fases de detección y prevención.

## 6.7.3 Proteger el código

1. Integrar las mejores prácticas de codificación segura para los procesos de desarrollo

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP) publicó una Guía rápida de referencia, que brinda una lista de comprobación que se puede integrar en el ciclo de vida de desarrollo. Está disponible en su sitio web.

## 6.7.4 Auditorías y análisis de vulnerabilidades periódicos

1. Realizar auditorías de los servidores y controlar los registros con periodicidad:  
Realizar la auditoría de los servidores con regularidad es importante en el ciclo de vida de la administración de la infraestructura de TI. Esto ayudará a asegurar que los requisitos mínimos de seguridad se cumplen siempre, los usuarios y los administradores cumplen con las políticas de seguridad. También permitirá identificar todos los problemas de seguridad que tienen que arreglarse o monitorearse, esto con el fin de mitigar a lo mínimo el riesgo que este latente en ese momento.
2. Analizar servidores en busca de vulnerabilidades: Para identificar las vulnerabilidades en el software y los paquetes instalados en los servidores, es importante realizar análisis de vulnerabilidades con frecuencia.

## **7. CONCLUSIONES Y RECOMENDACIONES**

## 7.1 CONCLUSIONES

Al realizar este análisis de riesgos se identificaron algunas complicaciones al no contar con las herramientas adecuadas para poder evaluar las vulnerabilidades en las plataformas de TI, que pueden depender de la configuración, desarrollo o implementación, por este motivo para evitar demoras e inconvenientes en los procesos de identificación de vulnerabilidades se debe optar por software más automatizado y de esta manera poder obtener resultados en menor tiempo.

Las herramientas de software libre son muy útiles para identificar vulnerabilidades en las plataformas de TI, pero requieren de muchos más trabajos manuales, lo que en dado momento puede aumentar el número de horas al realizar un análisis de riesgos.

El análisis de brecha de cumplimiento de controles de seguridad (GAP análisis) permitió medir el grado de madurez con que cuenta una organización en temas de seguridad de información, esto se da gracias a que el análisis de brecha está dividido por ítems los cuales evalúan en su totalidad a la compañía, después de esto se pudo concluir que para poner en marcha este plan de seguridad y seguir ciertos lineamientos es importante contar con el apoyo de la alta gerencia y adicional contar con la capacitación del personal en el tema sin importar el tamaño de la compañía.

El análisis de brecha de cumplimiento de controles de seguridad (GAP análisis), ayuda mucho a ver el panorama en el cual está la compañía, sumándole el análisis que se realizó a los activos, es muy útil al empezar a crear los planes de tratamiento ya que estos se pueden enfocar en lo que se ha identificado previamente, puesto que al tener el análisis de los activos y análisis de brecha los resultados son más notorios para plasmarlos con los controles o sugerencias que se deben hacer luego de este proceso.

Dentro de los planes de tratamiento se recomienda algún software libre, esto ya que dentro del estudio que se hizo durante la especialización estas herramientas son útiles para empresas pequeñas y con pocos recursos para invertir en seguridad, por lo tanto es un camino inicial para ellas.

La implementación de controles de acceso físicos o digitales reducirá las probabilidades que se genere algún tipo de acción, que atente contra la integridad de la información tanto física como digital. Cada empresa es un caso particular para lo cual debe existir un balance, ya que al implementar



demasiados controles se dificultara su administración y los usuarios finales tendrán inconvenientes para realizar el trabajo que requiere la organización.

Las aplicaciones que son desarrolladas en las empresas, están enfocadas en solucionar una necesidad de negocio, que se deben implementar en producción lo antes posible, sin tener en cuenta las posibles vulnerabilidades a las que se está expuesto por no incluir las mejores prácticas de seguridad de la información, ya sea por desconocimiento o por sobre costos de los proyectos.

Gran parte de los proyectos utilizan software libre o módulos desarrollados por terceros que a simple vista funcionan bien y cumplen con los requerimientos solicitados por el usuario, pero en estos requerimientos nunca están relacionados con el tema de la seguridad por lo tanto generan vulnerabilidades dentro de la aplicación comprometiendo la compañía al exponer información sensible.

Tradicionalmente se ve el problema de la seguridad de la información enfocado a temas de ataques informáticos, luego de realizar este trabajo se ve que la seguridad informática y de la información es un conjunto de componentes como son las personas, la tecnología, el ambiente, la ubicación, la política, las normativas o reglamentaciones donde todas las áreas del conocimiento hacen sinergia para gestionar adecuadamente la información.

Las empresas deberían realizar labores de sensibilización para que se cambie de alguna manera el pensamiento y la forma en la cual se administra la información personal y empresarial, resaltando que es eslabón más débil en la seguridad es el usuario.

Este trabajo ha permitido identificar los riesgos a los que está expuesta una organización utilizando herramientas como los diferentes análisis aplicados durante la investigación, los cuáles nos arrojaron resultados contundentes y de esta manera se pudieron proponer los planes de tratamiento que son las medidas de control que se deben implementar en la compañía.

## 7.2 RECOMENDACIONES

Las siguientes son las recomendaciones que se deben tener en cuenta para mejorar la seguridad en la información en el departamento de TI.

1. Implementar un plan de seguridad de la información el cual ayude a mejorar la situación actual de la compañía en cuanto a seguridad en su área de TI.
2. Revisar el Reporte de Vulnerabilidades para cerrar los puertos que actualmente no se utilizan y que pueden generar un riesgo para la organización.
3. Mejorar la seguridad física del área de servidores instalando una puerta que sirva como control de acceso, separando el área de servidores de las áreas comunes, adicionalmente mejorar la ventilación del área utilizando un rack.
4. Mejorar el procedimiento actual de backup, ya que al ser proceso manual que se ejecuta semanalmente y que en algún momento por olvido o múltiples compromisos puede fallar. Este procedimiento se podría mejorar utilizando un modelo de backup en la Nube.
5. En la actualidad la información que se envía y se transmite a través de la red de área local no va cifrada, lo que podría minimizar los riesgos generados por la interceptación de información para los servidores (planta telefónica, servidor de archivos, servidor web CRM y servidor de BD Mysql).
6. En el servidor WEB se recomienda Implementar mod\_security para combatir los ataques de SQL injection y Cross Site Script XSS. Mejorar la programación utilizando sanitización y validación de variables.
7. En la actualidad los usuarios tienen acceso a información que podría ser de carácter confidencial, y en dado caso podría ser robada, tanto para el CRM y los archivos de la red, para lo cual se recomienda mejorar la seguridad de acuerdo al tipo de usuario y perfil.
8. Mejorar la política de contraseñas, ya que las contraseñas no son cambiadas periódicamente, tampoco tienen una regla clara de caracteres que las hagan más seguras.
9. Revisión periódica de las UPS y de las fuentes de alimentación como la planta eléctrica, ya que esto puede generar falla en la disponibilidad del servicio y pueden verse afectados los usuarios remotos, adicionalmente un fallo eléctrico puede generar un daño físico en los discos de los servidores y por ende afectar la continuidad del negocio.
10. Asegurar el dispositivo Biométrico para acceso a la empresa, ya que es fácil de desmontarlo e ingresar a la empresa.

11. Definir un procedimiento para crear accesos a plataformas (CRM, Archivos, Biométrico), como también eliminación de accesos.
12. Mejorar la configuración del servidor de archivos.
13. Mejorar las configuraciones de los routers WIFI tanto en claves como su disposición física en la red.
14. Revisión periódica de los equipos de cómputo, troyanos y software que no debería estar instalado, se debe cumplir con las regulaciones y los licenciamientos.
15. Crear los planes de evacuación en caso de emergencia
16. Todos los funcionarios de la empresa deben tener el Anexo al contrato de trabajo que diga:  
Las herramienta como el Correo electrónico, Celulares, Equipos de cómputo y demás elementos entregados para la realización del trabajo serán catalogados como herramientas de trabajo, en las cuales estará prohibido almacenar información personal y podrán auditadas por el funcionario que la empresa autorice para su revisión.
17. Mejorar la auditoria del CRM para visualizar el trabajo de los funcionarios, que permitirá identificar la navegación de los funcionarios como de los asesores externos, que permitirá monitorear el comportamiento dentro del sistema.
18. En los desarrollos de aplicaciones utilizar un entorno de pruebas, que sea un servidor diferente al de producción.
19. En el desarrollo de aplicación utilizar las mejores prácticas OWASP.
20. Mejorar en los ítems deficientes que se encuentran en el análisis GAP.
21. Se recomienda que la compañía se alinee con ISO 27001, ya que luego del análisis de SOA se ven reflejadas muchos controles que aún no se ponen en práctica y que pueden ayudar a minimizar el impacto de la materialización de las amenazas detectadas durante este trabajo.
22. Al implementar las recomendaciones escritas en este documento no finalizara el proceso de la seguridad en la información en la empresa, debido a que este es un proceso que se debe realizar periódicamente y donde pueden aparecer otros riesgos o los mismos y se les debe dar un tratamiento nuevo, ya sea de prevención, mitigación o simplemente aceptación del riesgo.

## **BIBLIOGRAFÍA**

ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements.

ISO/IEC 27001:2005, Capítulo 1 Curso preparación CISM. Diplomado en Auditoría y Gestión de la Seguridad de la Información Gerencia de la seguridad de la información Auditoría interna de la norma.

ISO/IEC 27002:2013, Information technology - Security Techniques - Code of practice for information security controls.

ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management.

ISO 31000, Risk Management. Principles and Guidelines.

KAEO, Merike. Diseño de seguridad en redes. Madrid: Cisco Press, 2003.

OPPLIGER, Rolf. Security technologies for the World Wide Web. Boston: Artech House, 2003.

LAUDON, Kenneth. E-commerce: negocios, tecnología, sociedad. México: Person Education, 2009.

## CIBERGRAFÍA

“Seguridad de la información” consultado en  
<http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>

RUIZ L. Hernando. RESOLUCION 160-005326 Política de Seguridad de la información de la Superintendencia de Sociedades. 2008. Galdámez, Pablo, Seguridad Informática, julio 2003, Obtenido en:  
<http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf>

IZQUIERDO D, Fernando. La administración y los riesgos. EN: Maxitana C, Jennifer D. (Auditor en control de gestión). Tesis: Administración de riesgos de tecnología de información de una empresa del sector informático. Guayaquil – Ecuador: Escuela Superior politécnica del Litoral, 2005. P.39. Obtenido en:  
[http://www.cib.espol.edu.ec/Digipath/D\\_Tesis\\_PDF/D-33960.pdf](http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-33960.pdf)

VILCHES T, Martín. El riesgo [en line]. EN: Machuca C, John. (Magister en Contabilidad y Auditoría). Tesis Guía para la evaluación del sistema de riesgo operativo en la Cooperativa de Ahorro y Crédito Jardín Azuayo. Cuenca – Ecuador. Universidad de Cuenca, 2011. P.21. Obtenido en:  
<http://dspace.ucuenca.edu.ec/bitstream/123456789/2729/1/tm4487.pdf>

“Análisis de riesgo informático” consultado en  
[http://es.wikipedia.org/wiki/Análisis\\_de\\_riesgo\\_informático](http://es.wikipedia.org/wiki/Análisis_de_riesgo_informático)

“LEY 1273 DE 2009” consultado en  
<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

## **ANEXOS**

### **Anexo A GLOSARIO**

**ACEPTACIÓN DEL RIESGO:** admisión de la pérdida o ganancia proveniente de un riesgo particular.

**ACTIVO:** bienes o recursos de información que tienen valor para la compañía.

**AMENAZA:** origen, fuente potencial de afectación que causa un incidente no deseado y puede resultar en un daño a un sistema u organización y/o a sus activos.

**ANÁLISIS DE RIESGO:** uso sistemático de una metodología para la identificación fuentes o amenazas a las cuales están expuestos los activos, bienes o recursos de la compañía y estimar el riesgo.

**COMUNICACIÓN DEL RIESGO:** compartir la información acerca del riesgo entre las personas o área responsable que toma la decisión y otras partes interesadas.

**CONFIDENCIALIDAD:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**CONTROL:** es una forma de mitigar el impacto generado por la materialización de los riesgos existentes. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

**DECLARACIÓN DE APLICABILIDAD:** documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.

**DISPONIBILIDAD:** propiedad que determina que la información sea accesible y utilizable bajo solicitud por individuos, entidades o procesos autorizados.

**ESTIMACIÓN DEL RIESGO:** proceso de asignación de valores a la probabilidad y consecuencias de un riesgo.

**EVALUACIÓN DEL RIESGO:** proceso para determinar la importancia del riesgo con base en la comparación del mismo contra unos criterios dados.

**EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política de seguridad de la información, falla en controles y contramedidas, o que implica una situación desconocida que puede ser pertinente a la seguridad.

**EVITAR EL RIESGO:** decisión de la organización de no involucrarse en una situación de riesgo o tomar acciones para retirarse de dicha situación.

**GESTIÓN DEL RIESGO:** actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

**IDENTIFICACIÓN DEL RIESGO:** proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

**IMPACTO:** se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

**INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**INTEGRIDAD:** propiedad de salvaguardar la exactitud y estado completo de los activos.

**REDUCCIÓN DEL RIESGO:** acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

**RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN:** es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

**RIESGO INHERENTE:** es aquel riesgo que por su naturaleza no se puede separar de la situación donde se presenta. Es propio de las actividades que conlleva el proceso relacionado.

**RIESGO RESIDUAL:** nivel restante de riesgo después de su tratamiento.

**SEGURIDAD DE LA INFORMACIÓN:** preservación de la confidencialidad, integridad y disponibilidad de la información.

**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI:** parte del sistema de gestión global cuyo fin es establecer, implementar, operar, monitorear y mejorar la seguridad de la información.

**TRANSFERENCIA DEL RIESGO:** compartir con otra de las partes la pérdida (consecuencias negativas) de un riesgo.

**TRATAMIENTO DEL RIESGO:** proceso de selección e implementación de medidas para modificar el riesgo.

**VALORACIÓN DEL RIESGO:** proceso global de análisis y evaluación del riesgo.

VULNERABILIDAD: debilidad asociada con los procesos, recursos o infraestructura de una organización. Una vulnerabilidad frecuentemente aumenta la probabilidad de que se materialice una amenaza.

## **Anexo B REPORTE DE VULNERABILIDADES**

Las herramientas utilizadas para identificar las vulnerabilidades en los servidores de la Firma PINZÓN PINZÓN & ASOCIADOS ABOGADOS fueron NMAP bajo Windows y ZAP OWASP ya que son herramientas de libre distribución usadas en la seguridad informática como herramientas claves en la gestión.

La herramienta NMAP permite identificar los puertos y servicios que tiene en ejecución un servidor y que en dado momento podemos desinstalar o inhabilitar mejorando el funcionamiento del servidor y eliminando posibles problemas de seguridad.

La herramienta ZAP OWASP permite realizar pruebas de seguridad en las aplicaciones WEB, para identificar vulnerabilidad y realizar las respectivas correcciones ya sea en la programación de la aplicación o en la seguridad del servidor.

Antes de ejecutar este programa de seguridad se implementó el acceso por directorio lateral, para no incurrir en danos en la BD que se pudieran ocasionar.

Los servidores a Evaluar son 3:

1. Servidor de aplicaciones y de archivos ( Fenix Data- CRM 192.168.177.197)

Este servidor se encarga del aplicativo web FENIX – DATA- CRM (Gestión de Clientes, Facturación, Control de tiempo, Seguimientos, documentos, emails), tiene unas carpetas compartidas en la red vía Samba para las cuales se deberá mejorar los accesos y adicionalmente los recibe vía modem externo utilizando el programa Hylafax.

S.O. Centos 6.5, HP Xenon, 8 Gb Ram, 4 TB disco Raid 10

NMAP:



Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	open	http	Apache httpd 2.2.15 ((CentOS))
111	tcp	open	rpcbind	2-4 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: PPA)
443	tcp	open	http	Apache httpd 2.2.15
445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: PPA)
3306	tcp	open	mysql	MySQL 5.1.73
4559	tcp	open	hylafax	HylaFAX 6.0.6
8443	tcp	open	http	Apache httpd 2.2.15 ((CentOS))
10000	tcp	open	http	MiniServ 1.700 (Webmin httpd)
45968	tcp	open	status	1 (RPC #100024)

Como se puede observar en la imagen, existen unos servicios activos que se deberían bloquear, inhabilitar o desinstalar como son:

Puerto 10000: Se debe desinstalar el Swat de Samba

Puerto 111, 45968, 3306, 4559, 8443 bloquear acceso

Puerto 443 es para acceso remoto sin VPN a través de un usuario y contraseña, que se debe cambiar periódicamente, lo cual no se hace en la actualidad.

Las políticas de contraseñas debe implementarse, lo usuarios de acceso al servidor son los necesarios y suficientes.

## ZAP OWASP:

**Bienvenido al OWASP Zed Attack Pro**

ZAP es una herramienta para pruebas de penetración, de fácil uso y con múltiples opciones. Ten en cuenta que sólo debes atacar aplicaciones para las cuales se ha sido diseñado. Para probar una aplicación rápidamente, introduce la URL y presiona 'Atacar'.

URL a atacar:

Progreso:  Ataque completo - vea los problemas encontrados en la pestaña de Alertas.

Para un análisis más en profundidad de la prueba se debe explorar la aplicación. Si usted está usando Firefox 24.0 o superior puede usar 'Plug-in-Hack' para controlar el navegador.

**Alertas (6)**

- X-Frame-Options Header Not Set (14)
- Cookie set without HttpOnly flag (2)
- Password Autocomplete in browser (2)
- Private IP Disclosure (8)
- Web Browser XSS Protection Not Enabled (14)
- X-Content-Type-Options Header Missing (14)

Como se puede observar, existen 5 alertas que se deben controlar como son:

El autocompletar de los navegadores.

El Cross Site Script ya que se debería implementar el mod\_security para Apache.

Revisar las cabeceras de los programas, ya que en algunos no existe.  
Colocar en los programas la propiedad Intelectual de los mismos.  
Se debe definir Cookie como única y con los atributos de tiempo de expiración, adicionalmente en el “**php.ini**” se debe colocar la siguiente instrucción `session.cookie_httponly = True`.

En este servidor se encuentra la aplicación Fénix Data, por lo cual se recomienda que el entorno de desarrollo se implemente en otro servidor, y que los datos de desarrollo para pruebas no contengan información de la operación.

Se adjunta el informe del servidor como anexo.

NMAP 192.168.177.197.DOCX

ZAP OWASP 192.168.177.197.docx

ZAP 192.168.177.197.htm

## 2. Servidor Planta Telefónica - Asterisk ( 192.168.175.200)

Este servidor es una pequeña central telefónica Asterisk, el cual administra las llamadas y almacena los datos en una BD Mysql.  
S.O. Centos 6.5, HP Celeron, 4 Gb Ram, 2 TB, 2 tarjetas de red

NMAP:

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	open	http	Apache httpd 2.2.15 ((CentOS))
111	tcp	open	rpcbind	2-4 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: PPA)
443	tcp	open	http	Apache httpd 2.2.15 ((CentOS))
445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: PPA)
2000	tcp	open	cisco-sccp	
3306	tcp	open	mysql	MySQL (unauthorized)
4445	tcp	open	upnotifyp	
5038	tcp	open	asterisk	Asterisk Call Manager 1.3
8443	tcp	open	http	Apache httpd 2.2.15 ((CentOS))
49581	tcp	open	status	1 (RPC #100024)

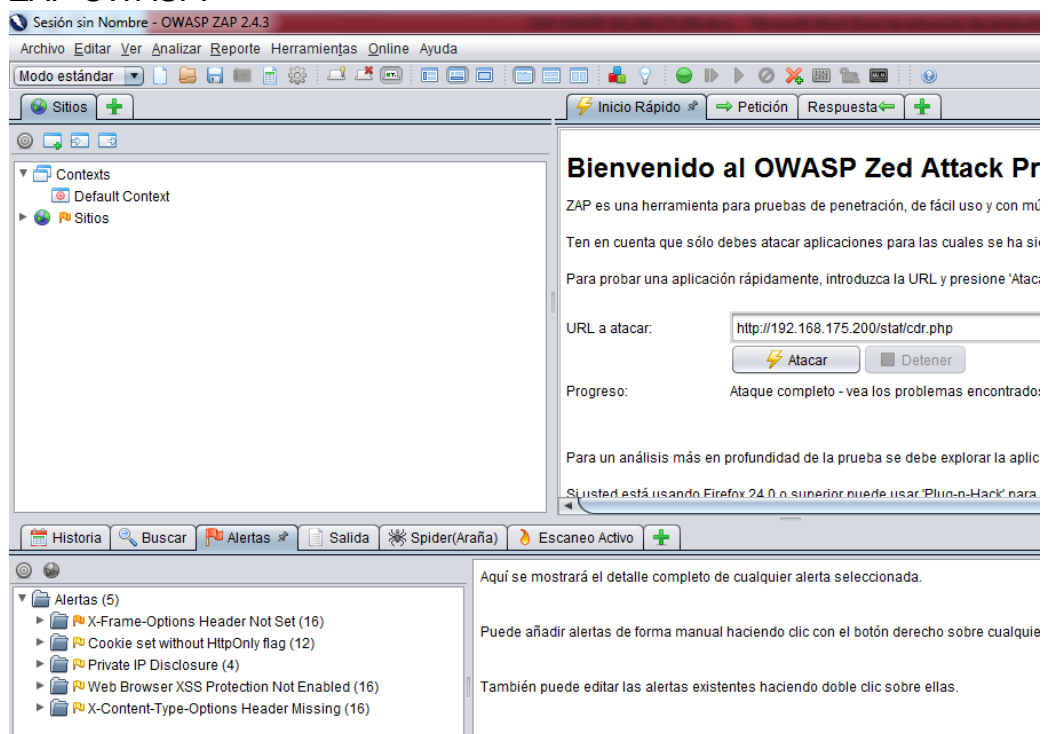
Como se observa en la imagen existen algunos servicios activos que se deben bloquear, deshabilitar o desinstalar.

Puerto 111, 3306, 8443, 49581 bloquear acceso

Puerto 2000 desinstalar servicio anteriores teléfonos IP que requerían configuración vía TFTP.

Puerto 4445 Puerto para mensajes de la planta Asterisk, no se utiliza en la actualidad.

## ZAP OWASP:



Como se puede observar, existen 5 alertas que se deben controlar como son:

El autocompletar de los navegadores.

El Cross Site Script ya que se debería implementar el mod\_security para Apache.

Revisar las cabeceras de los programas, ya que en algunos no existe.

Colocar en los programas la propiedad Intelectual de los mismos.

Se debe definir Cookie como única y con los atributos de tiempo de expiración, adicionalmente en el **"php.ini"** se debe colocar la siguiente instrucción `session.cookie_httponly = True`.

Se adjunta el informe del servidor como anexo.

NMAP 192.168.175.200.DOCX

ZAP OWASP 192.168.175.200.docx

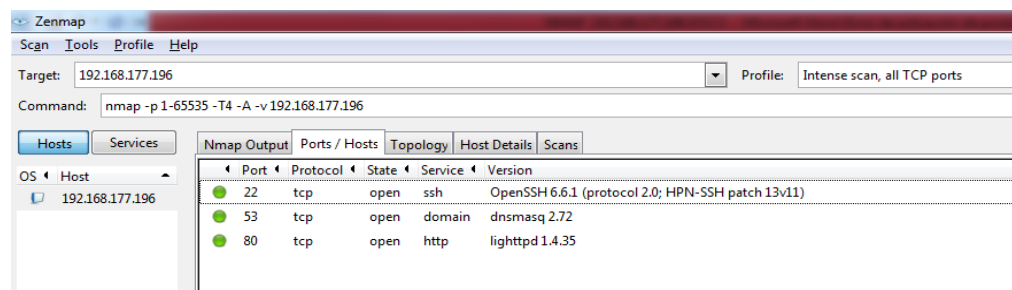
ZAP OWASP 192.168.175.200.htm

3. Servidor Firewall - PFSense ( 192.168.177.196 / 192.168.175.196)

Este servidor se encarga de administrar las conexiones a internet de la empresa, administra y controla las conexiones vía VPN.

S.O. freebsd en la distribución PfSense, HP Celeron, 4 Gb Ram, 2 TB, 3 tarjetas de red.

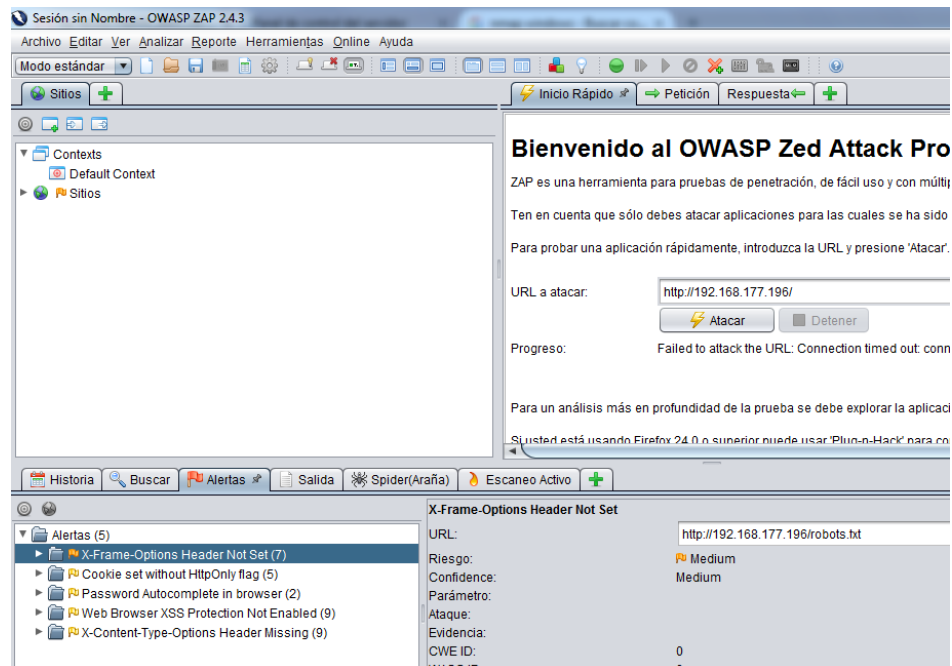
### NMAP:



Los servicios que están habilitados son los necesarios para la operación, pero sería importante que adicionalmente a este Firewall existiera un IPS o IDS para poder anticiparse o controlar los ataques que ponen en riesgo la continuidad del negocio.

Existe un procedimiento de alta y eliminación a las VPN, y adicionalmente se revisan periódicamente.

### ZAP OWASP:



Esta es una herramienta desarrollada como Firewall, pero posee vulnerabilidades en su aplicación de gestión.  
En el servidor Lighttpd, debería tener implementado el Mod\_security para añadir mayor seguridad.

Se adjunta el informe del servidor como anexo.  
NMAP 192.168.177.196.DOCX  
ZAP OWASP 192.168.177.196.docx  
ZAP OWASP 192.168.177.196.htm

### Anexo C DOCUMENTO DE DECLARACIÓN DE APLICABILIDAD (SOA)

Declaración de Aplicabilidad									
RL: Requerimientos legales, OC: obligaciones contractuales, RN/MP: requerimientos de negocio/mejores prácticas adoptadas, RER: resultados de evaluación de riesgos									
ISO 27001:2013 Controles			Controles Actuales	Observaciones (Justificación de exclusión)	Controles Seleccionados y Razones para Selección				Observaciones (Vista general de los objetivos de implementación)
					RL	OC	RN/MP	RER	
Cláusula	Sec.	Objetivo de Control/Control							
Políticas de la seguridad de la Información	5.1	Orientación de la dirección para la gestión de la seguridad de la información							
	5.1.1	Políticas para la seguridad de la información	X						
	5.1.2	Revisión de las políticas para seguridad de la información						X	
Organización de Seguridad de la Información	6.1	Organización Interna							
	6.1.1	Seguridad de la información Roles y responsabilidades	X						
	6.1.2	Separación de deberes	X						
	6.1.3	Contacto con las autoridades					X		
	6.1.4	Contacto con grupos de interés especial					X		
	6.1.5	Seguridad de la información en gestión de proyectos					X		
	6.2	Dispositivos móviles y teletrabajo							
	6.2.1	Política para dispositivos móviles						X	
	6.2.2	Teletrabajo	X						

Declaración de Aplicabilidad								
<b>RL:</b> Requerimientos legales, <b>OC:</b> obligaciones contractuales, <b>RN/MP:</b> requerimientos de negocio/mejores prácticas adoptadas, <b>RER:</b> resultados de evaluación de riesgos								
ISO 27001:2013 Controles			Controles	Observaciones	Controles			
			Actuales	(Justificación)				Observaciones (Visión general)
Seguridad de los recursos humanos	7.1	Antes de asumir el empleo						
	7.1.1	Selección	X					
	7.1.2	Términos y condiciones del empleo	X					
	7.2	Durante la ejecución del empleo						
	7.2.1	Responsabilidades de la dirección	X					
	7.2.2	Toma de conciencia, educación y formación en la seguridad de la información					X	
	7.2.3	Proceso disciplinario	X					
	7.3	Terminación y cambio de empleo						
	7.3.1	Terminación o cambio de responsabilidades de empleo				X		
Gestión de Activos	8.1	Responsabilidad por los activos						
	8.1.1	Inventario de activos	X					
	8.1.2	Propiedad de los activos	X					Se han definidos algunos, pero faltan
	8.1.3	Uso aceptable de los activos	X					
	8.1.4	Devolución de activos	X					
	8.2	Clasificación de la información						
	8.2.1	Clasificación de la información	X					
	8.2.2	Etiquetado de la información	X					

Declaración de Aplicabilidad									
RL: Requerimientos legales, OC: obligaciones contractuales, RN/MP: requerimientos de negocio/mejores prácticas adoptadas, RER: resultados de evaluación de riesgos									
ISO 27001:2013 Controles				Controles Actuales (Justificación)	Observaciones	Controles Seleccionados y Justificados			Observaciones (Vista general)
	8.2.3	Manejo de activos		X					
	8.3	Manejo de medios de soporte							
	8.3.1	Gestión de medios de soporte removibles		X				X	Si se realiza pero el procedimiento no es el adecuado
	8.3.2	Disposición de los medios de soporte		X				X	
	8.3.3	Transferencia de medios de soporte físicos		X				X	
Control de acceso	9.1	Requisitos del negocio para control de acceso							
	9.1.1	Política de control de acceso		X					
	9.1.2	Acceso a redes y a servicios en red		X					
	9.2	Gestión de acceso de usuarios							
	9.2.1	Registro y cancelación del registro de usuarios		X					
	9.2.2	Suministro de acceso de usuarios		X					
	9.2.3	Gestión de derechos de acceso privilegiado							X
	9.2.4	Gestión de información de autenticación secreta de usuarios							X
	9.2.5	Revisión de los derechos de acceso de usuarios						X	
	9.2.6	Cancelación o ajuste de los derechos de acceso		X					
	9.3	Responsabilidades de los usuarios							
	9.3.1	Uso de información de autenticación secreta							X



<b>Declaración de Aplicabilidad</b>									
<b>RL:</b> Requerimientos legales, <b>OC:</b> obligaciones contractuales, <b>RN/MP:</b> requerimientos de negocio/mejores prácticas adoptadas, <b>RER:</b> resultados de evaluación de riesgos									
ISO 27001:2013 Controles				Controles Actuales	Observaciones (Justificación)	Controles Seleccionados			
									Observaciones (Vista general)
	9.4	Control de acceso a sistemas y aplicaciones							
	9.4.1	Restricción de acceso a información		X					
	9.4.2	Procedimiento de conexión segura						X	
	9.4.3	Sistema de gestión de contraseñas		X				X	
	9.4.4	Uso de programas utilitarios privilegiados						X	
	9.4.5	Control de acceso a códigos fuente de programas		X					
Criptografía	10.1	Controles criptográficos							
	10.1.1	Política sobre el uso de controles criptográficos						X	
	10.1.2	Gestión de claves						X	
Seguridad Física y Ambiental	11.1	Áreas seguras							
	11.1.1	Perímetro de seguridad física		X				X	
	11.1.2	Controles físicos de entrada		X				X	
	11.1.3	Seguridad de oficinas, salones e instalaciones						X	
	11.1.4	Protección contra amenazas externas y ambientales						X	
	11.1.5	Trabajo en áreas seguras							NO APLICA
	11.1.6	Áreas de despacho y carga							NO APLICA
	11.2	Equipos							
	11.2.1	Ubicación y protección de los equipos						X	

Declaración de Aplicabilidad									
RL: Requerimientos legales, OC: obligaciones contractuales, RN/MP: requerimientos de negocio/mejores prácticas adoptadas, RER: resultados de evaluación de riesgos									
ISO 27001:2013 Controles				Controles	Observaciones	Controles			
				Actuales	(Justificación)	Seleccionados	Adaptados	Excluidos	Observaciones (Vista general)
	11.2.2	Servicios públicos de soporte		X					
	11.2.3	Seguridad del cableado		X					
	11.2.4	Mantenimiento de equipos		X					
	11.2.5	Retiro de activos		X					
	11.2.6	Seguridad de equipos y activos fuera del predio					X		
	11.2.7	Disposición segura o reutilización de equipos		X					
	11.2.8	Equipos de usuario desatendido						X	
	11.2.9	Política de escritorio limpio y pantalla limpia		X					
Seguridad de las operaciones	12.1	Procedimientos operacionales y responsabilidades							
	12.1.1	Procedimientos de operación documentados		X					
	12.1.2	Gestión de cambios		X					
	12.1.3	Gestión de capacidad		X					
	12.1.4	Separación de los ambientes de desarrollo, pruebas, y operacionales					X		
	12.2	Protección contra códigos maliciosos							
	12.2.1	Controles contra códigos maliciosos		X					
	12.3	Copias de respaldo							
	12.3.1	Copias de respaldo de la información		X			X		Se debería mejorar el procedimiento
	12.4	Registro y seguimiento							

Declaración de Aplicabilidad									
RL: Requerimientos legales, OC: obligaciones contractuales, RN/MP: requerimientos de negocio/mejores prácticas adoptadas, RER: resultados de evaluación de riesgos									
ISO 27001:2013 Controles				Controles Actuales	Observaciones (Justificación)	Controles Seleccionados			Observaciones (Visión general)
	12.4.1	Registro de eventos						X	
	12.4.2	Protección de la información de registro							X
	12.4.3	Registros del administrador y del operador							X
	12.4.4	Sincronización de relojes						X	X
	12.5	Control de software operacional							
	12.5.1	Instalación de software en sistemas operativos						X	X
	12.6	Gestión de la vulnerabilidad técnica							
	12.6.1	Gestión de las vulnerabilidades técnicas						X	
	12.6.2	Restricciones sobre la instalación de software						X	
	12.7	Consideraciones sobre auditorías de sistemas de información							
	12.7.1	Controles sobre auditorías de sistemas de información						X	
Seguridad de las comunicaciones	13.1	Gestión de la seguridad de redes							
	13.1.1	Controles de redes		X					
	13.1.2	Seguridad de los servicios de red		X					
	13.1.3	Separación en las redes		X					
	13.2	Transferencia de información							
	13.2.1	Políticas y procedimientos de transferencia de información							X
	13.2.2	Acuerdos sobre transferencia de información							X

<b>Declaración de Aplicabilidad</b>									
<b>RL:</b> Requerimientos legales, <b>OC:</b> obligaciones contractuales, <b>RN/MP:</b> requerimientos de negocio/mejores prácticas adoptadas, <b>RER:</b> resultados de evaluación de riesgos									
ISO 27001:2013 Controles				Controles	Observaciones	Controles			Observaciones
				Actuales	(Justificación)	Seleccionados	Excluidos	Excluidos	(Visión general)
	13.2.3	Mensajes electrónicos						X	
	13.2.4	Acuerdos de confidencialidad o de no divulgación		X					
Adquisición, desarrollo y mantenimiento de sistemas	14.1	Requisitos de seguridad de los sistemas de información							
	14.1.1	Análisis y especificación de requisitos de seguridad de la información		X					
	14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		X					
	14.1.3	Protección de transacciones de servicios de aplicaciones		X					
	14.2	Seguridad en los procesos de desarrollo y de soporte							
	14.2.1	Política de desarrollo seguro					X		
	14.2.2	Procedimientos de control de cambios en sistemas					X	X	
	14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones					X	X	
	14.2.4	Restricciones sobre cambios en los paquetes de software					X	X	
	14.2.5	Principios de organización de sistemas seguros					X	X	
	14.2.6	Ambiente de desarrollo seguro		X			X		
	14.2.7	Desarrollo contratado externamente							NO APLICA
	14.2.8	Pruebas de seguridad de sistemas					X	X	
	14.2.9	Prueba de aceptación de sistemas						X	
	14.3	Datos de prueba							
	14.3.1	Protección de datos de prueba					X		NO APLICA

Declaración de Aplicabilidad									
RL: Requerimientos legales, OC: obligaciones contractuales, RN/MP: requerimientos de negocio/mejores prácticas adoptadas, RER: resultados de evaluación de riesgos									
ISO 27001:2013 Controles				Controles	Observaciones	Controles			Observaciones
				Actuales	(Justificación)	Seleccionados	Excluidos	Excluidos	(Visión general)
Relaciones con los proveedores	15.1	Seguridad de la información en las relaciones con los proveedores							
	15.1.1	Política de seguridad de la información para las relaciones con proveedores					X	X	
	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores					X	X	
	15.1.3	Cadena de suministro de tecnología de información y comunicación					X	X	
	15.2	Gestión de la prestación de servicios de proveedores							
	15.2.1	Seguimiento y revisión de los servicios de los proveedores					X	X	
	15.2.2	Gestión de cambios a los servicios de los proveedores					X	X	
Gestión de incidentes de seguridad de la información	16.1	Gestión de incidentes y mejoras en la seguridad de la información							
	16.1.1	Responsabilidades y procedimientos	X				X		
	16.1.2	Informe de eventos de seguridad de la información					X	X	
	16.1.3	Informe de debilidades de seguridad de la información					X	X	
	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.					X	X	
	16.1.5	Respuesta a incidentes de seguridad de la información					X	X	
	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información					X	X	
	16.1.7	Recolección de evidencia					X	X	

Declaración de Aplicabilidad									
RL: Requerimientos legales, OC: obligaciones contractuales, RN/MP: requerimientos de negocio/mejores prácticas adoptadas, RER: resultados de evaluación de riesgos									
ISO 27001:2013 Controles			Controles	Observaciones	Controles				Observaciones
			Actuales	(Justificación)					(Visión general)
Aspectos de seguridad de la información de la gestión de continuidad de negocio	17.1	Continuidad de seguridad de la información							
	17.2.1	Planificación de la continuidad de la seguridad de la información					X	X	
	17.1.2	Implementación de la continuidad de la seguridad de la información					X	X	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información					X	X	
	17.2	Redundancias							
	17.2.1	Disponibilidad de instalaciones de procesamiento de información.					X	X	
Cumplimiento	18.1	Cumplimiento de requisitos legales y contractuales							
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	X						
	18.1.2	Derechos de propiedad intelectual	X						
	18.1.3	Protección de registros	X						
	18.1.4	Privacidad y protección de información de datos personales	X						
	18.1.5	Reglamentación de controles criptográficos					X	X	
	18.2	Revisiones de seguridad de la información							
	18.2.1	Revisión independiente de la seguridad de la información					X	X	
	18.2.2	Cumplimiento con las políticas y normas de seguridad	X				X		
	18.2.3	Revisión del cumplimiento técnico					X	X	

## **Anexo D FORMATO POLÍTICA CONTRASEÑAS**

### **Acta de Compromiso**

Para revisión de problemas en ambiente de Producción en la compañía, se han establecido claves de acceso a bases de datos, con el objeto de que se pueda leer únicamente la información o datos a los que se está autorizado.

En tal virtud me comprometo a cumplir las políticas de seguridad de datos que tiene implementadas la compañía.

### **Políticas**

1. Cualquier mal uso de este permiso para revisar las bases de datos o incumplimiento del procedimiento de seguridad de datos, será objeto de sanciones según las circunstancias.
2. La clave de acceso es personal e intransferible y debe ser cambiada cada 2 semanas por el responsable de la misma.
3. Está terminantemente prohibido que empleados o externos no autorizados accedan directamente a los datos, archivos o librerías para su lectura o modificación. Teniendo la responsabilidad absoluta la persona que suministre la clave de acceso para que se incumpla esta disposición.

### **DECLARACIÓN**

Declaro libre y voluntariamente que conozco las políticas de seguridad de claves de acceso a la base de datos en ambiente de producción de la compañía y declaro que haré buen uso de la clave que me ha sido asignada y acepto el establecimiento de las sanciones que la compañía estimare pertinente por el mal uso de la misma.

Fecha: \_\_\_\_\_

Nombre: \_\_\_\_\_

Cargo: \_\_\_\_\_

Firma: \_\_\_\_\_

Login: \_\_\_\_\_